AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

Volume LXXVII, Number 2
APRIL, 1955

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

CONTENTS

The AMERICAN JOURNAL OF MATHEMATICS appears four times yearly.

The subscription price of the JOURNAL is $8.50 in the U. S.; $8.75 in Canada; and $9.00 in other foreign countries. The price of single numbers is $2.50.

Manuscripts intended for publication in the JOURNAL should be sent to Professor AUREL WINTNER, The Johns Hopkins University, Baltimore 18, Md.

Subscriptions to the JOURNAL and all business communications should be sent to THE JOHNS HOPKINS PRESS, BALTIMORE 18, MARYLAND, U. S. A.

Entered as second-class matter at the Baltimore, Maryland, Postoffice, acceptance for mailing at special rate of postage provided for in Section 1103, Act of October 3, 1917, Authorized on July 3, 1918.

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

ON THE GALOIS COHOMOLOGY OF UNRAMIFIED EXTENSIONS OF FUNCTION FIELDS IN ONE VARIABLE.*

By Y. KAWADA and J. TATE.

I. The Abstract Case.

Let k be an algebraic function field in one variable over an algebraicly closed constant field k_0. Let K/k be a finite normal unramified extension with Galois group $G = G(K/k)$. Our aim is to investigate the cohomology groups of the Galois group G with coefficients in various multiplicative groups associated with K. Some of the coefficient groups which we consider, and our notations for them, are the following:

$D(K) =$ the group of divisors of K;

$P(K) =$ the group of principal divisors of K;

$E(K) = D(K)/P(K) =$ the group of divisor classes of K;

$U =$ the group of all roots of unity in k_0;

$E^*(K) = \mathrm{Hom}(E(K), U) =$ the group of all homomorphisms of $E(K)$ into U.

We omit K in these notations when considering a fixed field K.

A rough outline of our program is the following. We first show $H^r(G, E) \approx H^{r+2}(G, U)$ for all r, by using three exact coefficient group sequences linking E to U. By duality it follows then that $H^r(G, E^*) \approx H^{r-2}(G, Z)$, at least in case the characteristic p does not divide the order of G. This result is exactly parallel to the main theorem of class field theory which states $H^r(G, C) \approx H^{r-2}(G, Z)$ if G is a group of automorphisms of a number field with idèle class group C. Therefore, casting the group E^* of divisor class characters in the role of the idèle class group, we can produce a pseudo class field theory for the extensions under consideration. We develop the parallel with ordinary class field thory in some detail, and discuss the relation of our pseudo class field theory to the simpler Kummer theory. In the second half of the paper, we consider the classical case in which the ground field is the

* Received August 4, 1954.

field of complex numbers. Then the divisor class group E has a natural locally compact topology, and it turns out that its Pontrjagin character group $\hat{E}$ can be used instead of E^*. Viewing 1-cycles on the Riemann surface as characters of the group of divisor classes of degree 0, we can give an explicit topologico-analytic description of the fundamental generator of $H^2(G, \hat{E})$, and can show that the reciprocity law of our pseudo class field theory is the mapping which attaches to a 1-cycle on the ground surface the corresponding covering transformation of an abelian unramified covering surface.

The cohomology groups which we will be using are those associated with the operation of a *finite* group G on a G-module A. They are denoted by $H^r(G, A)$ and are defined, and in general non-trivial, for all integers r, positive and negative. The negative dimensional cohomology groups are isomorphic to the ordinary homology groups of G in A. The group $H^0(G, A)$ may be identified with A^G/NA, the factor group of elements $a \in A$ which are invariant under the operations of G, modulo elements of the form $a = Nb = \prod_{\sigma \in G} b^\sigma$ for $b \in A$. The basic properties of these groups are developed in Chapter XII of [1]. The main fact, which justifies the introduction of negative dimensional groups, is that an exact sequence of coefficient modules of the type $0 \to A' \to A \to A'' \to 0$ leads to an exact cohomology sequence

$$\cdots \to H^r(G, A) \to H^r(G, A'') \to H^{r+1}(G, A') \to H^{r+1}(G, A) \to \cdots$$

which extends all the way from $r = -\infty$ to $r = +\infty$. Furthermore, cup products are defined in all dimensions, positive and negative: if A and B are G-paired into C, there is induced a pairing of $H^r(G, A)$ and $H^s(G, B)$ into $H^{r+s}(G, C)$ for *all* r, s. This pairing has all the usual properties of a cup product. Finally, we mention that $H^r(G, A) = 0$ for all r if A is G-regular; that is, if $A = \sum_{\sigma \in G} B^\sigma$ is the direct sum of translations of a subgroup $B \subset A$. After these preliminary remarks, we now return to the field theoretic situation described in the first paragraph.

In order to determine the cohomology groups $H^r(G, E(K))$ we consider three natural exact sequences:

$$\{1\} \to P \to D \to E \to \{1\}, \tag{1}$$

$$\{1\} \to k_0^* \to K^* \to P \to \{1\}, \tag{2}$$

$$\{1\} \to U \to k_0^* \to k_0^*/U \to \{1\}. \tag{3}$$

In each of these three sequences, one of the modules has trivial cohomology groups in all dimensions. In the first sequence we have $H^r(G, D) = 0$ for

all r, because D is G-regular. The G-regularity of D follows from our assumptions that K/k is unramified and that the constant field k_0 is algebraicly closed. Namely, if for each prime divisor $\mathfrak{p}$ of k we select a fixed prime $\mathfrak{P}$ of K dividing $\mathfrak{p}$, then the other primes of K dividing $\mathfrak{p}$ are those of the form $\mathfrak{P}^\sigma$, for $\sigma \in G$, and these are distinct. Consequently, if D_1 is the subgroup of D generated by the selected $\mathfrak{P}$'s, then D is the direct product of the translations $D_1{}^\sigma$ of the subgroup D_1, and is therefore G-regular. In the second sequence (2) we have $H^r(G, K^*) = 0$ for all r. This fact depends only on the constant field $k_0{}^*$ being algebraicly closed. By Tsen's theorem we know that every element of k^* is a norm from K^*, which means that $H^0(G, K^*) = 0$. Coupling this with the fact that $H^1(G, K^*) = 0$, and noting that the same holds if G is replaced by any subgroup G_1 of G, we see that the G-module K^* has the property that its cohomology groups in two successive dimensions are trivial for all subgroups of G. From this it follows that they are trivial in all dimensions [7], [9]. For positive r the triviality of $H^r(G, K^*)$ has been noted by Nakayama and Hochschild [5]. In the third sequence (3) we have $H^r(G, k_0{}^*/U) = 0$ for all r, because $k_0{}^*/U$ has unique divisibility. Since k_0 is algebraicly closed, every element of $k_0{}^*$ has an n-th root, for every natural number n, and this n-th root is uniquely determined modulo U.

Using these cases of trivial cohomology groups in the cohomology sequences associated with our exact sequences of coefficient groups we obtain three isomorphisms:

$$(1') \qquad \delta\colon H^r(G, E) \approx H^{r+1}(G, P),$$

$$(2') \qquad \delta\colon H^r(G, P) \approx H^{r+1}(G, k_0{}^*),$$

$$(3') \qquad i\colon H^r(G, U) \approx H^r(G, k_0{}^*).$$

Putting these together we find finally:

$$(4) \qquad i^{-1}\delta\delta\colon H^r(G, E) \approx H^{r+2}(G, U).$$

G operates simply on the group of roots of unity U, and U has a simple structure which depends only on the characteristic p of $k_0{}^*$. Thus in the situation we are considering—unramified extension and algebraicly closed constant field—the cohomology of G with coefficients in the divisor classes depends only on G and on the characteristic, not at all on the fields K and k.

The result we have obtained is remotely suggestive of class field theory. In class field theory, there is associated with each field K of a certain type a multiplicative group $A(K)$ such that, if G is a finite group of automorphisms

of K, then G operates on $A(K)$ and we have $H^r(G, A(K)) \approx H^{r-2}(G, Z)$ for all r, where Z denotes the additive group of rational integers under trivial operation by G (cf. [6], [7], [9]). In local class field theory, $A(K)$ is the multiplicative group of the local field K. In global class field theory, $A(K)$ is the idèle class group of the number field K. In our present situation, where K is an unramified extension of the function field K, we can also find suitable coefficient groups $A(K)$ whose cohomology is like that of class field theory. To this effect we put $A(K) = E^*(K)$, where $E^*(K) = \mathrm{Hom}(E(K), U)$ is the group of all homomorphisms of the divisor class group of K into the roots of unity U. We call these homomorphisms characters of E and denote them by $\chi: E \to U$. If $\sigma: K \to K^\sigma$ is an isomorphism of K relative to k, we can define a corresponding isomorphism $\sigma: E^*(K) \to E^*(K^\sigma)$ by putting $\chi^\sigma(a^\sigma) = \chi(a)$ for $a \in E(K)$. The rule $(\chi^\sigma)^\tau = \chi^{(\tau\sigma)}$ is then obvious, and it follows that any group G of automorphisms of K/k operates in a natural way on $E^*(K)$.

To determine the cohomology groups $H^r(G, E^*(K))$ we need only use the duality theorem for the cohomology groups of finite groups which we now explain: Let W be a fixed abelian group on which G operates simply (W will be U in our applications). For any G-module X, let $X^* = \mathrm{Hom}(X, W)$. Then X^* and X are G-paired into W, and if $\phi \in H^r(G, X^*)$, the cup product multiplication by ϕ gives a map $\bar{\phi}$ of $H^{-1-r}(G, X)$ into $H^{-1}(G, W)$. Since $H^{-1}(G, W)$ can be identified with a subgroup of W, we may view this map $\bar{\phi}$ as an element of $(H^{-1-r}(G, X))^* = \mathrm{Hom}(H^{-1-r}(G, X), W)$. The duality theorem states that if W is divisible, then the map $\phi \to \bar{\phi}$ is an isomorphism: $H^r(G, X^*) \approx (H^{-1-r}(G, X))^*$; see, for example, [1] or [7].

In our field theoretic situation, U is divisible, because every root of unity has an n-th root for every natural number n, and this n-th root is again a root of unity. Therefore using (4) together with the duality theorem we find

$$H^r(G, E^*) \approx (H^{-1-r}(G, E))^* \approx (H^{1-r}(G, U))^*. \tag{5}$$

If Z is the additive group of integers with G operating simply, then the natural isomorphism $Z^* = \mathrm{Hom}(Z, U) \approx U$ is a G-isomorphism. Consequently, using the duality theorem again we find

$$H^{1-r}(G, U) \approx H^{1-r}(G, Z^*) \approx (H^{r-2}(G, Z))^*. \tag{6}$$

Combining (5) and (6) we obtain

$$H^r(G, E^*) \approx (H^{r-2}(G, Z))^{**}. \tag{7}$$

Now $H^{r-2}(G, Z)$ is a finite abelian group. If Y is any finite abelian group,

the natural duality map $Y \to Y^{**}$ is an epimorphism (homomorphism onto). This follows in the usual way from the simple structure of U; namely, U contains at most one subgroup U_n of order n for each natural number n. In case the characteristic p is zero the map is an isomorphism, $Y \approx Y^{**}$, because then U_n exists for each n. In case $p > 0$, the map $Y \to Y^{**}$ has as kernel the p-primary part of Y (elements of p-power order), because then U_n exists only for n prime to p. Combining the natural map $H^{r-2}(G, Z) \to (H^{r-2}(G, Z))^{**}$ with the inverse of the isomorphism (7) we obtain therefore an epimorphism,

$$f: H^{r-2}(G, Z) \to H^r(G, E^*) \tag{8}$$

which is obviously canonical, and whose kernel is the p-primary part of $H^{r-2}(G, Z)$, p being the characteristic, and 0-primary part meaning the identity subgroup.

Having proved the existence of this epimorphism f, we can now describe it in more concrete terms. Reviewing the considerations of the preceding paragraphs, we see that f is simply the adjoint of the isomorphism (4)

$$i^{-1}\delta\delta: H^{-1-r}(G, E) \approx H^{1-r}(G, U),$$

with respect to the cup product duality. In other words, if $\zeta \in H^{r-2}(G, Z)$, then $f(\zeta) \in H^r(G, E^*)$ is uniquely determined by the property that

$$f(\zeta) \cdot \alpha = \zeta \cdot (i^{-1}\delta\delta\alpha), \tag{9}$$

for all $\alpha \in H^{-1-r}(G, E)$, where the dot denotes cup product multiplication. From this description of f, we can easily establish the rule $f(\zeta_1 \cdot \zeta) = f(\zeta_1) \cdot \zeta$ for any two integral cohomolgy classes ζ and ζ_1, if we use the fact that multiplication by an integral cohomology class ζ commutes with the natural cohomological operations i and δ. Namely, if α is any cohomology class over E of the appropriate dimension for determining $f(\zeta_1 \cdot \zeta)$ we have:

$$f(\zeta_1 \cdot \zeta) \cdot \alpha = \zeta_1 \cdot \zeta \cdot (i^{-1}\delta\delta\alpha) = \zeta_1 \cdot (i^{-1}\delta\delta(\zeta \cdot \alpha)) = f(\zeta_1) \cdot \zeta \cdot \alpha,$$

and since this is true for all α we can conclude $f(\zeta_1 \cdot \zeta) = f(\zeta_1) \cdot \zeta$, as stated.

Now putting $\zeta_1 = 1 \in H^0(G, Z)$, the unit element in the cohomology ring of G, and defining the fundamental two-dimensional class $\alpha^* \in H^2(G, E^*)$ by $\alpha^* = f(1)$, we see finally that $f(\zeta) = \alpha^* \cdot \zeta$. In other words, our canonical epimorphism (8), $H^{r-2}(G, Z) \to H^r(G, E^*)$, is obtained by multiplication with a fundamental two-dimensional class in E^*, just as in class field theory.

Our next task is to give an explicit characterization of the fundamental class $\alpha^* = f(1)$ by means of the standard 2-cocycles $\chi_{\sigma,\tau}$, which represent it.

Putting $\zeta = 1$ in (9) and applying the isomorphism i, we see that α^* is uniquely determined by the property

$$i(\alpha^* \cdot \alpha) = \delta\delta\alpha, \tag{10}$$

for all $\alpha \in H^{-3}(G, E)$. What we shall now do is simply write out formula (10) in terms of standard cochains. The fundamental class α^* will be represented by a standard 2-cocycle $\chi_{\sigma,\tau}$, which is a function $(\sigma, \tau) \to \chi_{\sigma,\tau}$ from $G \times G$ to E^* satisfying the identity $(\delta\chi)_{\rho,\sigma,\tau} = \chi^{\rho}{}_{\sigma,\tau}\chi^{-1}{}_{\rho\sigma,\tau}\chi_{\rho,\sigma\tau}\chi^{-1}{}_{\rho,\sigma} = 1$. Any (-3)-dimensional class α of G in E will be represented by a standard (-3)-cocycle $a_{\sigma,\tau}$, which is a function $(\sigma, \tau) \to a_{\sigma,\tau}$ from $G \times G$ to E satisfying the identity $(\delta a)_{\tau} = \prod_{\sigma} a^{\sigma^{-1}}{}_{\sigma,\tau} a^{-1}{}_{\sigma,\sigma^{-1}\tau} a_{\tau,\sigma} = 1$. The (-1)-dimensional class $\alpha^* \cdot \alpha$ is then described by the single element $\epsilon = \prod_{\sigma,\tau} \chi_{\sigma,\tau}(a_{\sigma,\tau})$, which is an n-th root of unity ($n = [K : k]$ = order of G). The left hand side of (10) is therefore the (-1)-dimensional class in $k_0{}^*$ determined by ϵ. To compute the right hand side of (10) we must choose divisors $\mathfrak{A}_{\sigma,\tau}$ in K representing the divisor classes $a_{\sigma,\tau}$. The coboundary of the (-3)-cochain $\mathfrak{A}_{\sigma,\tau}$ consists of principal divisors (A_τ), $A_\tau \in K^*$ such that

$$(A_\tau) = (\delta\mathfrak{A})_\tau = \prod_{\sigma} \mathfrak{A}^{\sigma^{-1}}{}_{\sigma,\tau}\mathfrak{A}^{-1}{}_{\sigma^{-1},\sigma\tau}\mathfrak{A}_{\tau,\sigma} \qquad (\text{in } D(K)). \tag{11}$$

The standard (-2)-cocycle (A_τ) then represents the (-2)-dimensional class $\delta\alpha \in H^{-2}(G, P)$, and the coboundary of the K^*-valued (-2)-cochain A_τ will be equal to the unique (-1)-cocycle ϵ which represents the class $\delta\delta\alpha \in H^{-1}(G, k_0{}^*)$:

$$\epsilon = \delta A = \prod_{\tau} A_\tau{}^{\tau^{-1}-1} \qquad (\text{in } K^*). \tag{12}$$

(ϵ is unique because G operates simply on $k_0{}^*$, so there are no (-1)-dimensional coboundaries.)

The standard two cocycles $\chi_{\sigma,\tau}$ of G in E^* which represent the fundamental class α^* are therefore those with the following property: Given any set of functions $A_\tau \in K^*$, and divisors $\mathfrak{A}_{\sigma,\tau} \in D(K)$ such that (11) holds, then the following equation holds:

$$\prod_{\sigma,\tau} \chi_{\sigma,\tau}(\mathfrak{A}_{\sigma,\tau}) = \prod_{\tau} A_\tau{}^{\tau^{-1}-1}. \tag{13}$$

Here the divisor class characters $\chi_{\sigma,\tau}$ are understood to be applied to divisors $\mathfrak{A}_{\sigma,\tau}$ in the obvious way.

To show that the parallel between our present situation and class field theory is complete, we must consider the interrelations among different fields. In class field theory, whenever a field k is a subfield of a field K, the associated

module $A(k)$ is a submodule of $A(K)$; more precisely, there is a canonical monomorphism $i_{k/K}: A(k) \to A(K)$, which is usually viewed as an inclusion. In our case the role of this monomorphism is played by the conorm, $N^*_{k/K}: E^*(k) \to E^*(K)$, which is the dual of the norm, $N_{K/k}: E(K) \to E(k)$, and is defined by $(N^*_{k/K}\chi)(a) = \chi(N_{K/k}a)$ for $\chi \in E^*(k)$ and $a \in E(K)$. This conorm N^* is indeed a monomorphism, because the norm N is an epimorphism on divisor classes. In fact, the norm is an epimorphism even on the divisors themselves; a prime in the ground field is the norm of any one of the primes in the extension field dividing it, because the constant field is algebraicly closed. Of course the conorm monomorphism is transitive in the sense that $N^*_{k/K} = N^*_{k_1/K}N^*_{k/k_1}$, whenever $k \subset k_1 \subset K$.

There is on more property of the inclusion map $i_{k/K}: A(k) \to (K)$ which is crucial in class field theory. This can be expressed by saying that the fundamental theory of Galois Theory holds for the modules A. Precisely what we mean is this: If K/k is a normal extension with group $G = G(K/k)$, then the image of $A(k)$ in $A(K)$ consists exactly of the elements of $A(K)$ which are left fixed by the operation of G, or in a formula $i_{k/K}(A(k)) = (A(K))^G$. To show that the conorm has this property, i. e.,

$$N^*_{k/K}(E^*(k)) = (E^*(K))^G, \tag{14}$$

we note first that the left hand side is obviously included in the right. To show the converse, let $\chi \in (E^*(K))^G$. We wish to find a $\psi \in E^*(k)$ such that $\chi = N^*\psi$, that is, such that

$$\chi(a) = \psi(Na), \tag{15}$$

for all $a \in E(K)$. To this effect, we observe that the ψ we are looking for will be completely defined by (15) if it exists at all, because Na runs over the whole of $E(k)$ as a runs over $E(K)$. Therefore, we try to use (15) as a definition of ψ. This will work, provided we can show that $\chi(a) = 1$ whenever $Na = 1$, and this of course is where the assumption that χ is invariant under G must come in. Suppose therefore that $Na = 1$. Let $\mathfrak{A}$ be a divisor in K representing the divisor class a. Since $Na = 1$, $N\mathfrak{A}$ is principal, and there exists a function $\alpha \in k$ such that $N\mathfrak{A} = (\alpha)$. Since $H^0(G, K^*) = 0$ there exists a function $A \in K$ such that $NA = \alpha$. It follows that $N(\mathfrak{A}A^{-1}) = (1)$, and consequently there exist divisors $\mathfrak{B}_\sigma$ in K, $\sigma \in G$, such that

$$\mathfrak{A}A^{-1} = \prod_\sigma \mathfrak{B}_\sigma{}^{\sigma-1}.$$

(This follows from $H^{-1}(G, D) = 0$, but can easily be seen directly if we

recall that K/k is assumed unramified.) Finally, letting $b_\sigma \in E(K)$ be the divisor class of the divisor $\mathfrak{B}_\sigma$ and going over to divisor classes, we find

$$a = \prod_\sigma b_\sigma^{\sigma-1}.$$

Since χ is invariant under G we have $\chi(b_\sigma{}^\sigma) = \chi(b_\sigma)$ for all σ and consequently $\chi(a) = 1$, which is what we were trying to prove.

There is of course a map of divisor class characters which goes in the opposite direction to the conorm. We call it the norm and denote it by $N_{K/k}: E^*(K) \to E^*(k)$. We define this norm as the dual of the natural injection $i_{k/K}: E(k) \to E(K)$ of divisor classes of the subfield k into those of the extension K, that is,

$$(N\chi)(a) = \chi(ia), \tag{16}$$

for $\chi \in E^*(K)$ and $a \in E(k)$. The justification for the term norm for this map rests in the formula

$$N^*(N\chi) = \prod_\sigma \chi^\sigma, \tag{17}$$

which states that $N\chi$ is essentially—i. e., when imbedded in $E^*(K)$ by the conorm becomes—the product of the conjugates of χ. To prove (17) we simply write, for $a \in E(K)$,

$$\begin{aligned}(N^*(N\chi))(a) = (N\chi)(Na) = \chi(iNa) = \chi(\prod_\sigma a^{\sigma^{-1}}) \\ = \prod_\sigma \chi(a^{\sigma^{-1}}) = \prod_\sigma \chi^\sigma(a) = (\prod_\sigma \chi^\sigma)(a).\end{aligned}$$

From (14) and (17) we see that the conorm N^* induces a natural isomorphism of the group of divisor class character norm residues of the ground field k, $E^*(k)/N(E^*(K))$, onto the factor group of divisor class characters of K which are invariant under G, modulo those which are products of conjugates. This latter factor group may of course be identified with the 0-dimensional cohomology group $H^0(G, E^*(K))$. Therefore we have

$$H^0(G, E^*(K)) \approx E^*(k)/N(E^*(K)). \tag{18}$$

If K/k is abelian, of degree $n = [K:k]$ prime to p, and if we use the natural isomorphism

$$H^{-2}(G, Z) \approx G, \tag{19}$$

then we can interpret the case $r = 0$ of our natural epimorphism (8) as an isomorphism

$$f: G \approx E^*(k)/N(E^*(K)) \tag{20}$$

(isomorphism because of the assumption that G has no elements of order p). This isomorphism f is the analog of the reciprocity law isomorphism of class field theory. In class field theory, an explicit formula for this isomorphism is given by the Nakayama map associated with a fundamental 2-cocycle. The same holds in our present case, because the Nakayama map is simply an explicit formula for the cup product of an element of $H^{-2}(G, Z)$ which corresponds to $\rho \in G$ under the isomorphism (19), with the fundamental class, and our map f is defined by such a product. Therefore, as an explicit formula for (20) we have, for $\rho \in G$,

$$f(\rho) = \psi_\rho \pmod{N(E^*(K))}, \tag{21}$$

if $\psi_\rho \in E^*(k)$ is defined by

$$N^*\psi_\rho = \prod_\sigma \chi_{\sigma,\rho}, \tag{22}$$

$\chi_{\sigma,\rho}$ being a fundamental 2-cocycle.

The norm group $N(E^*(K))$ can easily be described directly; it consists of those characters ψ of $E^*(k)$ which are trivial on the kernel of the injection map $i: E(k) \to E(K)$, i. e., which satisfy the condition $\psi(i^{-1}(1)) = 1$. Indeed, this condition is obviously necessary and sufficient for the existence of a character χ_0 on the subgroup $i(E(k))$ of $E(K)$ such that $\psi = \chi_0 i$; and since any such χ_0 can be extended to a character of $E(K)$ with the aid of Zorn's lemma and the divisibility of U, we see that our condition is necessary and sufficient for the existence of $\chi \in E^*(K)$, such that $\psi = \chi i$, i. e., $\psi = N\chi$.

From what we have said it follows that to determine the coset of a character $\psi \in E^*(k)$ modulo the norm group $N(E^*(K))$ is simply to give the values of ψ on the subgroup $i^{-1}(1)$ of $E(k)$. This shows what we must do in order to give an explicit formula for the reciprocity law isomorphism (20): for each $\rho \in G$ and each $c \in i^{-1}(1)$ we must calculate the root of unity $\psi_\rho(c)$, where ψ_ρ is defined by equation (22), $\chi_{\sigma,\rho}$ being a fundamental 2-cocycle. The result is the following: Let $\mathfrak{c}$ be a divisor in k representing the class of c. Since $ic = 1$, $\mathfrak{c}$ becomes principal in K, i. e., $\mathfrak{c} = (B)$ with $B \in K^*$. Then

$$\psi_\rho(c) = B^{\rho^{-1}-1}. \tag{23}$$

To prove this, let $\mathfrak{B}$ be a divisor in K such that $\mathfrak{c} = N\mathfrak{B}$. In K this equation reads

$$(B) = \prod_\sigma \mathfrak{B}^{\sigma^{-1}}.$$

This last equation can be put in the form of equation (11) if we define the (-1)-cochain $A_\tau \in K^*$ and the (-2)-cochain $\mathfrak{A}_{\sigma,\tau} \in D(K)$ by $A_\tau = 1$ or

$A_\tau = B$ according as $\tau \neq \rho$ or $\tau = \rho$ and $\mathfrak{A}_{\sigma,\tau} = 1$ or $\mathfrak{A}_{\sigma,\tau} = \mathfrak{B}$ according as $\tau \neq \rho$ or $\tau = \rho$. The resulting equation (13) then reads

$$\prod_\sigma \chi_{\sigma,\rho}(\mathfrak{B}) = B^{p^{-1}-1}.$$

Comparing this with (22) and noting $N\mathfrak{B} = \mathfrak{c} \in c$, we see that (23) holds as contended.

Of course the proper interpretation of the result which we have obtained is simply to view it as giving the relationship between our pseudo class field theory of unramified abelian extensions of degree prime to p, and the Kummer theory of such extensions. Using the Kummer theory, one easily proves the appropriate existence theorem for our pseudo class field theory, namely, a subgroup X of $E^*(k)$ is the norm subgroup of some class field K/k if and only if there exists a subgroup Y of $E(k)$ of finite order n prime to p, such that X consists of all characters trivial on Y. The class field is then obtained by taking for each element of Y a representative divisor $\mathfrak{c}$, and then extracting the n-th roots of elements $\gamma \in k^*$ for which $(\gamma) = \mathfrak{c}^n$.

In order to complete the discussion of the parallel between our situation and class field theory, we must consider the relations between the fundamental 2-dimensional classes in different extensions. For these considerations we drop the assumption that the extensions are abelian.

Let $\bar{k} \subset k \subset K$ with $K/\bar{k}$ normal unramified, but $k/\bar{k}$ not necessarily normal. We wish to prove that the restriction to K/k of the fundamental class $\bar{\alpha}^*$ of $K/\bar{k}$ is equal to the fundamental class α^* of K/k. For the proof we let $\bar{G} = G(K/\bar{k})$ and $G = G(K/k)$, so that G is a subgroup of $\bar{G}$. Let elements $A_\tau \in K^*$ and divisors $\mathfrak{A}_{\sigma,\tau} \in D(K)$ be given satisfying equation (11) for $\sigma, \tau \in G$. Extend the definition of these cochains A and $\mathfrak{A}$ to the big group $\bar{G}$ by defining $A_\tau = 1$ for $\tau \notin G$ and $\mathfrak{A}_{\sigma,\tau} = (1)$ for σ or $\tau \notin G$. Then equation (12) still holds if G is replaced by $\bar{G}$, i. e., if the product is taken over all of $\bar{G}$ instead of over the subgroup G. If $\chi = \chi_{\sigma,\tau}$ is a fundamental 2-cocycle for the extension $K/\bar{k}$, then we obtain from (13)

$$\prod_{\sigma,\tau \in G} \chi_{\sigma,\tau}(\mathfrak{A}_{\sigma,\tau}) = \prod_{\sigma,\tau \in \bar{G}} \chi_{\sigma,\tau}(\mathfrak{A}_{\sigma,\tau}) = \prod_{\tau \in \bar{G}} A_\tau^{\tau^{-1}-1} = \prod_{\tau \in G} A_\tau^{\tau^{-1}-1}.$$

This shows that the restriction of χ to the subgroup G is a fundamental 2-cocycle for the extension K/k as contended.

Next, suppose $k \subset \bar{K} \subset K$ with both extensions normal and unramified. Let $m = [K : \bar{K}]$. We wish to prove that the inflation of the fundamental class of $\bar{K}/k$ is equal to the m-th power of the fundamental class of K/k. Let $\bar{G} = G(\bar{K}/k)$ and $G = G(K/k)$ so that $\bar{G}$ is a factor group of G. Let

functions A_τ and divisors $\mathfrak{A}_{\sigma,\tau}$ be given satisfying equation (11) for $\sigma, \tau \in G$. Viewing the elements of $\bar{G}$ as cosets in G, and denoting them by s, t, etc., define

$$\bar{A}_t = \prod_{\tau \in t} N_{K/\bar{K}} A_\tau; \qquad \bar{\mathfrak{A}}_{s,t} = \prod_{\sigma \in s,\ \tau \in t} N_{K/\bar{K}} \mathfrak{A}_{\sigma,\tau}.$$

Then from the fact that $\bar{K}/k$ is normal, one sees easily that the quantities $\bar{A}_t$ and $\mathfrak{A}_{s,t}$ satisfy the condition (11) for the extension $\bar{K}/k$, and furthermore,

$$\prod_t \bar{A}_t^{t^{-1}-1} = N_{K/\bar{K}}\left(\prod_\tau A_\tau^{\tau^{-1}-1}\right) = \left(\prod_\tau A_\tau^{\tau^{-1}-1}\right)^m, \tag{24}$$

because $\prod_\tau A_\tau^{\tau^{-1}-1} \in k_0^*$. Consequently, if $\bar{\chi} = \bar{\chi}_{s,t}$ is a fundamental 2-cocycle for $\bar{K}/k$ we obtain from (13) and (24)

$$\begin{aligned}\prod_\tau (A_\tau^{\tau^{-1}-1})^m &= \prod_{s,t} \bar{\chi}_{s,t}(\bar{\mathfrak{A}}_{s,t}) = \prod_{s,t} \prod_{\sigma \in s,\ \tau \in t} \bar{\chi}_{s,t}(N_{K/\bar{K}} \mathfrak{A}_{\sigma,\tau}) \\ &= \prod_{s,t} \prod_{\sigma \in s,\ \tau \in t} (N^*_{\bar{K}/K} \bar{\chi}_{s,t})(\mathfrak{A}_{\sigma,\tau}) = \prod_{\sigma,\tau \in G} (\operatorname{infl} \bar{\chi})_{\sigma,\tau}(\mathfrak{A}_{\sigma,\tau}),\end{aligned}$$

where $\operatorname{infl} \bar{\chi}$ is the inflation to G of $\bar{\chi}$. Since the m-th power of the usual left hand side occurs in this equation, we conclude that $\operatorname{infl} \bar{\chi}$ represents the m-th power of the fundamental class of K/k as contended.

II. The Classical Case.

We turn now to the classical case in which the constant field k_0 is the field of complex numbers. In addition to our old notations which will still be used in the present section we introduce the following new ones:

$D_0(K)$ = the group of divisors of degree 0 of K;

$E_0(K)$ = the group of divisor classes of degree 0 of K;

T = the group of unimodular complex numbers (one dimensional torus group);

$g(K)$ = genus of K;

$R(K)$ = the Riemann surface of K;

$H_1(K) = H_1(R(K), Z)$ = the 1-dimensional homology group of $R(K)$ with integer coefficients.

As is well known, $H_1 \approx Z^{2g}$ is a free abelian group on $2g$ generators, $E_0 \approx T^{2g}$ is a $2g$-dimensional torus group, and there is a natural duality between H_1 and E_0 in the sense of Pontrjagin. Giving E_0 the compact

topology of T^{2g}, we can extend this topology to E in a unique way such that the factor group $E/E_0 \approx Z$ is discrete, i. e., such that E_0 is an open subgroup of E. Then E is a locally compact group and from the exact sequence

$$\{1\} \to E_0 \to E \to Z \to \{1\}, \tag{1}$$

we obtain the dual exact sequence

$$\{1\} \leftarrow H_1 \leftarrow \hat{E} \leftarrow T \leftarrow \{1\}, \tag{2}$$

which shows that the Pontrjagin character group $\hat{E}$ of E has an open compact subgroup T, with the factor group isomorphic to the discrete group $H_1 \approx Z^{2g}$. Of course the exact sequences (1) and (2) split; if a_1 is any fixed divisor class of degree 1, then any divisor class can be written uniquely in the form aa_1^{ν} with $a \in E_0$, $\nu \in Z$, so we have $E \approx E_0 \times Z \approx T^{2g} \times Z$ and accordingly $\hat{E} \approx H_1 \times T \approx Z^{2g} \times T$. These direct product decompositions are topological as well as algebraic, but they are not canonical since they depend on the choice of a_1.

The advantage of the classical case, which we are now discussing over the algebraic case discussed in the preceding section, is that we can use the topological character group $\hat{E}$, whose simple structure we have just described, in place of the algebraic character group E^*. E^* was defined to be the group of all homomorphisms of E into the group of roots of unity U; $E^* = \mathrm{Hom}(E, U)$. $\hat{E}$ is the group of continuous homomorphisms of E into T; $\hat{E} = \mathrm{Cont\,Hom}(E, T)$. Both these groups are subgroups of the group $\mathrm{Hom}(E, T)$ of all homomorphisms of E into T. The first thing to remark is that all the facts we have proven in **I** about $E^* = \mathrm{Hom}(E, U)$ are true for $\mathrm{Hom}(E, T)$ as well, because the only properties of U which we used in **I** are possessed also by T, namely: (i) k_0^*/T has unique divisibility; (ii) T is divisible; and (iii) T has exactly one subgroup of order n for each natural number n. Next, in order to show that the cohomology groups with coefficients in $\mathrm{Hom}(E, T)$ are the same as those with coefficients in $\hat{E} = \mathrm{Cont\,Hom}(E, T)$, we will prove that the factor group $\mathrm{Hom}(E, T)/\mathrm{Cont\,Hom}(E, T)$ has unique divisibility. Since $E \approx T^{2g} \times Z$ is a direct product of T's and a Z, it suffices to prove the statement for the factors T and Z separately instead of for E itself. Z is no problem; being discrete, its homomorphisms are the same as its continuous homomorphisms. Concerning T we must prove: (a) For each natural number n, the homomorphisms $f: T \to T$ can be written in the form $f = g^n\phi$, where ϕ is continuous (divisibility of the factor group $\mathrm{Hom}(T, T)/\mathrm{Cont\,Hom}(T, T)$); and (b) If the n-th power of a homomorphism $g: T \to T$ is continuous, then g itself is continuous (uniqueness of the divisibility).

To prove (a), consider the group U_n of n-th roots of unity. A homomorphism $f: T \to T$ carries U_n into itself, and since U_n is cyclic, there exists an integer m such that $f(\epsilon) = \epsilon^m$ for $\epsilon \in U_n$. Define $\phi(\lambda) = \lambda^m$ for all $\lambda \in T$. Then $f(\epsilon) = \phi(\epsilon)$ for $\epsilon \in U_n$, so we can define a homomorphism $g: T \to T$ by $g(\lambda) = f(\sqrt[n]{\lambda})/\phi(\sqrt[n]{\lambda})$, this last quantity being independent of the choice of the n-th root. Hence $g^n(\lambda) = g(\lambda^n) = f(\lambda)/\phi(\lambda)$, or $f = g^n\phi$ as contended. Now consider statement (b). If g^n is continuous, then $g^n(\lambda) = \lambda^m$ for some integer m, because the only continuous homomorphisms of T into T are of this form. For $\epsilon \in U_n$ we find $g^n(\epsilon) = 1 = \epsilon^m$. Hence n divides m, say $m = nl$. It follows for any $\lambda \in T$ that $g(\lambda^n) = g^n(\lambda) = (\lambda^n)^l$, and since $T^n = T$, this implies $g(\lambda) = \lambda^l$ for all λ. Therefore g is continuous as contended.

Suppose now that our field K is a finite normal unramified extension of k with Galois group $G = G(K/k)$. Then, according to the remarks we have just made, we obtain an isomorphism

$$f: H^{r-2}(G, Z) \approx H^r(G, \hat{E}(K)) \tag{3}$$

of the same type as the isomorphism (8) of part I. Just as in the algebraic case, this isomorphism is given by the cup product with the canonical generator of $H^2(G, \hat{E})$. Soon we shall give a topologico-analytic description of this canonical 2-dimensional class. But first let us make a few remarks about the cohomology of G with coefficients in the homology group $H_1(K)$. The exact sequence (2) gives rise to the exact cohomology sequence

$$\cdots \to H^r(G, \hat{E}) \to H^r(G, H_1) \to H^{r+1}(G, T) \to H^{r+1}(G, \hat{E}) \to \cdots. \tag{4}$$

Using (3) together with $\delta: H^r(G, T) \approx H^{r+1}(G, Z)$, we can reinterpret (4) as

$$\cdots \to H^{r-2}(G, Z) \to H^r(G, H_1) \to H^{r+2}(G, Z) \to H^{r-1}(G, Z) \to \cdots. \tag{5}$$

This exact sequence (5)gives us some information about the groups $H^r(G, H_1)$. However, the problem of $H^r(G, H_1)$ can be viewed as a purely topological problem, and we should point out that an exact sequence of the same type as (5) can be obtained by standard topological methods. To this effect we forget about the analytic structure of the Riemann surfaces and simply view $R(K)$ as a finite regular unramified covering of $R(k)$ with covering transformation group G. By taking a cellular decomposition of $R(k)$ and lifting it up to the covering surface $R(K)$, we obtain a decomposition of $R(K)$ in which the cells are permuted by G, no cell being left fixed by any transformation other than the identity. Therefore in the associated chain complex

$$\cdots \to 0 \to C_2 \xrightarrow{\partial} C_1 \xrightarrow{\partial} C_0 \to 0 \to \cdots, \tag{6}$$

the chain groups C_r are free G-modules; and of course the boundary homomorphism δ is a G-homomorphism. Letting Z_j, B_j, and H_j denote the groups of j-cycles, j-boundaries, and j-homology classes in this complex, we can break the complex up into four exact sequences:

$$0 \to H_2 \xrightarrow{i} C_2 \xrightarrow{\partial} B_1 \to 0, \tag{7}$$

$$0 \to B_1 \xrightarrow{i} Z_1 \to H_1 \to 0, \tag{8}$$

$$0 \to Z_1 \xrightarrow{i} C_1 \xrightarrow{\partial} B_0 \to 0, \tag{9}$$

$$0 \to B_0 \xrightarrow{i} C_0 \to H_0 \to 0, \tag{10}$$

where i is the inclusion map. Now consider the cohomology groups associated with the operation of G on these modules. Since the C_j are G-free, and G is finite, we have $H^r(G, C_j) = 0$ for $j = 0, 1, 2$. Since $H_2 \approx Z \approx H_0$ we obtain from (7), and from (9) and (10), the isomorphisms

$$\delta_{(7)} : H^{r-1}(G, B_1) \approx H^r(G, H_2) \approx H^r(G, Z),$$

$$\delta_{(9)}\delta_{(10)} : H^{r-2}(G, Z) \approx H^{r-2}(G, H_0) \approx H^r(G, Z_1).$$

If we insert these results about B_1 and Z_1 in the following exact cohomology sequence associated with (8),

$$\cdots \to H^r(G, Z_1) \to H^r(G, H_1) \to H^{r+1}(G, B_1) \to H^{r+1}(G, Z_1) \to \cdots, \tag{11}$$

then we obtain an exact sequence which is of exactly the same form as (5), and which is presumably identical with (5), save possibly for the signs of the mappings. However, since this topological approach is a digression from our main line of thought, we will not enter further into the matter here.

In order to describe explicitly the canonical duality between H_1 and E_0 which we have used in the discussion above, we will make use of certain abelian differentials of the third kind which are attached to divisors of degree 0. If $\mathfrak{A} = \prod \mathfrak{P}^{\nu_\mathfrak{P}}$, $\sum \nu_\mathfrak{P} = 0$, is a divisor of degree 0, then the corresponding differential is denoted symbolically by $d \log \mathfrak{A}$ and is uniquely characterized by the following two properties: (i) At each point $\mathfrak{P} \in R$, $d \log \mathfrak{A}$ has a simple pole with residue $\nu_\mathfrak{P} =$ order of $\mathfrak{A}$ at $\mathfrak{P}$ (a simple pole with residue 0 is no pole at all!) (ii) All periods of $d \log \mathfrak{A}$ are pure imaginary. One method of showing the existence of these differentials is the following. The Riemann-Roch theorem guarantees the existence of a differential satisfying condition (i), because $\sum \nu_\mathfrak{P} = 0$. Its local periods are then integral multiples of $2\pi i$,

so condition (ii) is now merely a condition on the global periods. Since there exists a unique differential of first kind whose $2g$ basic global periods have arbitrarily prescribed real parts, we can correct our original differential of the third kind by one of the first so that condition (ii) is satisfied. From the characterization of these differentials by properties, it is clear that the rule

$$d\log(\mathfrak{A}\mathfrak{B}) = d\log\mathfrak{A} + d\log\mathfrak{B} \qquad (\mathfrak{A}, \mathfrak{B} \in D_0) \tag{12}$$

holds, and furthermore, if $\mathfrak{A} = (A)$ is the divisor of a function A, then

$$d\log\mathfrak{A} = d\log A = dA/A. \tag{13}$$

We appeal to (12) and (13) for justification of our somewhat unconventional notation $d\log\mathfrak{A}$.

If $\mathfrak{B}$ is a 1-chain on the surface R, and $\mathfrak{A}$ a divisor of degree 0, none of whose poles or zeros lie on the boundary of $\mathfrak{B}$, we define the symbol

$$(\mathfrak{B}, \mathfrak{A}) = \exp\int_{\mathfrak{B}'} d\log\mathfrak{A}, \tag{14}$$

where $\mathfrak{B}'$ is any 1-chain homologous to $\mathfrak{B}$ which avoids the singularities of $d\log\mathfrak{A}$. $\mathfrak{B}'$ can be obtained by deforming the cells of $\mathfrak{B}$ slightly, keeping their end points fixed. Since the local periods of $d\log\mathfrak{A}$ are integral multiples of $2\pi i$, the right side of (14) is independent of the choice of $\mathfrak{B}'$. The following rules for our symbol are evident from the definition

$$(\mathfrak{B}_1 + \mathfrak{B}_2, \mathfrak{A}) = (\mathfrak{B}_1, \mathfrak{A})(\mathfrak{B}_2, \mathfrak{A}), \tag{15}$$

$$(\mathfrak{B}, \mathfrak{A}_1\mathfrak{A}_2) = (\mathfrak{B}, \mathfrak{A}_1)(\mathfrak{B}, \mathfrak{A}_2). \tag{16}$$

Furthermore, if σ is a one-to-one conformal map of R on R, then we have

$$(\sigma\mathfrak{B}, \mathfrak{A}^\sigma) = (\mathfrak{B}, \mathfrak{A}), \tag{17}$$

because σ viewed as an integral substitution changes $\mathfrak{B}$ into $\sigma\mathfrak{B}$ and $d\log A$ into a differential with the characterizing properties of $d\log(\mathfrak{A}^\sigma)$, hence into $d\log(\mathfrak{A}^\sigma)$. Finally, if $A \in K^*$ is a function and the boundary of $\mathfrak{B}$ is $\partial\mathfrak{B} = \sum \nu_{\mathfrak{Q}}\mathfrak{Q}$, then we see from (13) that

$$(\mathfrak{B}, (A)) = A \mid_{\partial\mathfrak{B}} = \prod_{\mathfrak{Q}} (A(\mathfrak{Q}))^{\nu_{\mathfrak{Q}}}. \tag{18}$$

Let us now consider the symbol $(\Gamma, \mathfrak{A})$ for a 1-cycle, Γ. It is defined for all $\mathfrak{A} \in D_0$ because $\partial\Gamma$ is empty. Of course it depends only on the homology class $\bar{\Gamma}$ of Γ, and from (18) we see that it depends only on the divisor class $\bar{\mathfrak{A}}$ of $\mathfrak{A}$. Since the periods of $d\log\mathfrak{A}$ are pure imaginary $(\Gamma, \mathfrak{A})$ has absolute value 1, i. e., $(\Gamma, \mathfrak{A}) \in T$. Therefore the symbol $(\bar{\Gamma}, \bar{\mathfrak{A}}) = (\Gamma, \mathfrak{A})$ is a pairing

of H_1 and E_0 into T. In fact,, the discrete group H_1 and the compact group E_0 are dual under this pairing (see Weyl [2] or Igusa [3]). In the proof of the duality it is necessary to use the so-called theorem of interchange of argument and parameter to obtain a formula for $(\Gamma, \mathfrak{A})$ in terms of differentials of the first kind. Namely, if $\mathfrak{A} = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_m\mathfrak{Q}_1^{-1}, \mathfrak{Q}_2^{-1} \cdots \mathfrak{Q}_m^{-1}$ is any divisor of degree 0, the interchange shows that

$$(\Gamma, \mathfrak{A}) = \exp 2\pi i \mathcal{R}\{\sum_{j=1}^{m} \int_{\mathfrak{Q}_j}^{\mathfrak{P}_j} dw_\Gamma\},$$

where dw_Γ is the uniquely determined differential of the first kind such that

$$\mathcal{R} \int_{\Gamma'} dw_\Gamma = \text{intersection number of } \Gamma' \text{ and } \Gamma \text{ for all cycles } \Gamma'.$$

We can now describe the divisor class characters $\chi \in \hat{E}$ explicitly. As usual, we will sometimes view χ as a divisor character which is trivial on principal divisors, writing $\chi(\mathfrak{A}) = \chi(\bar{\mathfrak{A}})$ if $\bar{\mathfrak{A}}$ is the class of the divisor $\mathfrak{A}$. Let us select a prime divisor $\mathfrak{P}$, to be kept fixed during the rest of the discussion, so that an arbitrary divisor can be written uniquely in the form $\mathfrak{A}\mathfrak{P}^s$ with $\mathfrak{A} \in D_0$, $s \in Z$. Then if Γ is any 1-cycle, and λ any complex number of absolute value 1, we can define a character χ by the formula

$$\chi(\mathfrak{A}\mathfrak{P}^s) = (\Gamma, \mathfrak{A})\lambda^s. \tag{19}$$

We shall use the notation $\chi = \chi(\Gamma, \lambda)$ to refer to this character. Every character is of this form. The number $\lambda = \chi(\mathfrak{P})$ is uniquely determined by χ, as is the homology class $\bar{\Gamma}$ of Γ. The maps in the exact sequence (2), $T \to \hat{E} \to H_1$, are given by $\lambda \to \chi(0, \lambda)$ and $\chi(\Gamma, \lambda) \to \bar{\Gamma}$.

Suppose now that our field K is a normal unramified extension of k with Galois group $G = G(K/k)$. We contend that the automorphisms $\rho \in G$ operate on characters according to the rule

$$(\chi(\Gamma, \lambda))^\rho = \chi(\rho\Gamma, \lambda\,(\Gamma, \mathfrak{P}^{\rho^{-1}-1})). \tag{20}$$

Indeed from (17) we see that both sides of (20) yield the same value when applied to $\mathfrak{A} \in D_0$. The remaining computation

$$\chi^\rho(\mathfrak{P}) = \chi(\mathfrak{P}^{\rho^{-1}}) = \chi(\mathfrak{P})\chi(\mathfrak{P}^{\rho^{-1}-1}) = \lambda\,(\Gamma, \mathfrak{P}^{\rho^{-1}-1}),$$

shows that (20) is correct.

We can now give an explicit description of a fundamental 2-cocycle $\chi_{\sigma,\tau}$. Let $\mathfrak{O}$ be a fixed base point on the surface $R(K)$, none of whose conjugates $\mathfrak{O}^\sigma$, $\sigma \in G$, coincides with the point $\mathfrak{P}$. For each $\sigma \in G$, select a fixed path B_σ running from $\mathfrak{O}$ to $\mathfrak{O}^\sigma$. Then for each pair of elements $\sigma, \tau \in G$ the chain

$$\Gamma_{\sigma,\tau} = \mathrm{B}_\sigma + \sigma\mathrm{B}_\tau - \mathrm{B}_{\sigma\tau} \tag{21}$$

is a cycle, and as function of σ, τ, $\Gamma_{\sigma,\tau}$ is a standard 2-cocycle of G in the group of cycles. We contend that by suitable choice of numbers $\lambda_{\sigma,\tau} \varepsilon T$ we will obtain a fundamental 2-cocycle of the form

$$\chi_{\sigma,\tau} = \chi(\Gamma_{\sigma,\tau}, \lambda_{\sigma,\tau}). \tag{22}$$

Leaving the choice of the numbers $\lambda_{\sigma,\tau}$ open for the moment, we compute the coboundary of $\chi_{\sigma,\tau}$ by means of (20), obtaining

$$(\delta\chi)_{\rho,\sigma,\tau} = ((\delta\Gamma)_{\rho,\sigma,\tau},\ (\delta\lambda)_{\rho,\sigma,\tau}(\Gamma_{\sigma,\tau}, \mathfrak{P}^{\rho^{-1}-1})).$$

Since $\delta\Gamma = 0$, the condition on the λ's for $\chi_{\sigma,\tau}$ to be a cocycle is simply

$$(\delta\lambda)_{\rho,\sigma,\tau} = (\Gamma_{\sigma,\tau}, \mathfrak{P}^{\rho^{-1}-1})^{-1}. \tag{23}$$

To define the numbers $\lambda_{\sigma,\tau}$ we use the following notation: if z is any non-zero complex number, we put $\text{u.p.}z = z/|z|$ and call this the "unimodular part" of z. Putting

$$\lambda_{\sigma,\tau} = \text{u.p.}(\mathrm{B}_\tau, \mathfrak{P}^{\rho^{-1}-1}) = \exp(i\vartheta \int_{\mathrm{B}_\tau} d\log(\mathfrak{P}^{\sigma^{-1}-1})), \tag{24}$$

we find

$$(\delta\lambda)_{\rho,\sigma,\tau} = \text{u.p.}(\mathrm{B}_\tau, \mathfrak{P}^{\sigma^{-1}-1})(\mathrm{B}_\tau, \mathfrak{P}^{(\rho\sigma)^{-1}-1})^{-1}(\mathrm{B}_{\sigma\tau}, \mathfrak{P}^{\rho^{-1}-1})(\mathrm{B}_\sigma, \mathfrak{P}^{\rho^{-1}-1})^{-1}.$$

Combining the first two terms on the right and using rule (1$'$) gives

$$\begin{aligned}(\delta\lambda)_{\rho,\sigma,\tau} &= \text{u.p.}(\sigma\mathrm{B}_\tau, \mathfrak{P}^{\rho^{-1}-1})^{-1}\ \ (\mathrm{B}_{\sigma,\tau}, \mathfrak{P}^{\rho^{-1}-1})(\mathrm{B}_\sigma, \mathfrak{P}^{\rho^{-1}-1})^{-1} \\ &= \text{u.p.}(\Gamma_{\sigma,\tau}, \mathfrak{P}^{\rho^{-1}-1})^{-1}.\end{aligned}$$

Since $\Gamma_{\sigma,\tau}$ is a cycle, a symbol of the form $(\Gamma_{\sigma,\tau}, \mathfrak{A})$ is unimodular, and we can drop the u.p. Therefore (23) is satisfied, and our 2-cochain $\chi_{\sigma,\tau}$ is a 2-cocycle.

It is a straightforward matter to check by means of the criterion contained in formulas (11) and (13) of the first half of this paper that $\chi_{\sigma,\tau}$ is a fundamental 2-cocycle. We write the divisor (-3)-cochain in the form $\mathfrak{A}_{\sigma,\tau}\mathfrak{P}^{s_{\sigma,\tau}}$ with $\mathfrak{A}_{\sigma,\tau} \varepsilon D_0$, $s_{\sigma,\tau} \varepsilon Z$. Denoting the function (-2)-cochain as usual by A_τ, equation (I, 11) takes the form

$$(\mathrm{A}_\tau) = \prod_{\sigma \varepsilon G} \mathfrak{A}^{\sigma^{-1}}{}_{\sigma,\tau}\mathfrak{A}^{-1}{}_{\sigma^{-1},\sigma\tau}\mathfrak{A}_{\tau,\sigma}\mathfrak{P}^{\kappa}, \tag{25}$$

where κ stands for the (unprintable) exponent $\sigma^{-1}s_{\sigma,\tau} - s_{\sigma^{-1},\sigma\tau} + s_{\tau,\sigma}$. Assuming this, we must then show

$$\prod_{\sigma,\tau} \chi_{\sigma,\tau}(\mathfrak{A}_{\sigma,\tau}\mathfrak{P}^{s_{\sigma,\tau}}) = \prod_{\tau} A_\tau{}^{\tau^{-1}-1}. \tag{26}$$

After two preliminary remarks, it will turn out that (26) follows from a

straightforward computation. First, taking the degrees of the divisors equated in (25) we find $\sum_{\sigma} (s_{\sigma,\tau} - s_{\sigma^{-1},\sigma\tau} + s_{\tau,\sigma}) = 0$. Subtracting this quantity from the exponent κ of $\mathfrak{P}$ in (25) we obtain (25) in the simpler form:

$$(25') \qquad (A_\tau) = \prod_{\sigma \in G} \mathfrak{A}^{\sigma^{-1}}{}_{\sigma,\tau} \mathfrak{A}^{-1}{}_{\sigma^{-1},\sigma\tau} \mathfrak{A}_{\tau,\sigma} \mathfrak{P}^{(\sigma^{-1}-1)s_{\sigma,\tau}}.$$

Secondly, we remark that it is no loss of generality to assume that the divisors $\mathfrak{A}_{\sigma,\tau}$ have no zeros or poles at the places $\mathfrak{O}^\sigma$, $\sigma \in G$, so that the symbols of type $(\mathfrak{B}_\rho, \mathfrak{A}_{\sigma,\tau})$ are defined. This follows from the fact that the (-3)-cochain $\mathfrak{A}_{\sigma,\tau}\mathfrak{P}^{s_{\sigma,\tau}}$ serves to represent a divisor class (-3)-cocycle, and consequently each $\mathfrak{A}_{\sigma,\tau}$ may be changed by an arbitrary principal divisor.

Now to prove (26) we write

$$\prod_{\sigma,\tau} \chi_{\sigma,\tau} (\mathfrak{A}_{\sigma,\tau}\mathfrak{P}^{s_{\sigma,\tau}}) = \prod_{\sigma,\tau} (\Gamma_{\sigma,\tau}, \mathfrak{A}_{\sigma,\tau}) \lambda_{\sigma,\tau}{}^{s_{\sigma,\tau}}$$

$$= \text{u.p.} \prod_{\sigma,\tau} (\sigma\mathfrak{B}_\tau, \mathfrak{A}_{\sigma,\tau}) (\mathfrak{B}_{\sigma\tau}, \mathfrak{A}_{\sigma,\tau})^{-1} (\mathfrak{B}_\sigma, \mathfrak{A}_{\sigma,\tau}) (\mathfrak{B}_\tau, \mathfrak{P}^{(\sigma^{-1}-1)s_{\sigma,\tau}}).$$

In view of the product over σ and τ we can change the subscripts so that all symbols have $\mathfrak{B}_\tau$ in the left hand argument. Doing this, combining the right hand sides and using (25′) to carry out the product over σ we obtain simply u.p. $\prod_\tau (\mathfrak{B}_\tau, (A_\tau))$. Since $\partial\mathfrak{B}_\tau = \mathfrak{O}^\tau - \mathfrak{O}$ we have then by (18),

$$\text{u.p.} \prod_\tau A_\tau(\mathfrak{O}^\tau) A_\tau^{-1}(\mathfrak{O}) = \text{u.p.} \prod_\tau A_\tau{}^{\tau^{-1}-1}(\mathfrak{O}) = \prod_\tau A_\tau{}^{\tau^{-1}-1}$$

because the function $\prod_\tau A_\tau{}^{\tau^{-1}-1}$ is a constant of absolute value 1 (even a root of unity), and is therefore identically equal to the unimodular part of its value at the base point $\mathfrak{O}$. This concludes the proof that $\chi_{\sigma,\tau}$ is a fundamental 2-cocycle.

Now let K be an arbitrary finite extension of k, not necessarily normal. We wish to discuss the relations between characters, cycles, etc. of k, and those of K. For this purpose, we will use lower case letters to denote objects associated with k, the corresponding capitals denoting corresponding objects in K. The surface $R(K)$ is a finite unramified covering of $R(k)$; let π be the projection map of $R(K)$ on $R(k)$. For any point $\mathfrak{Q} \in R(K)$, $\pi\mathfrak{Q}$ is the point on $R(k)$ below $\mathfrak{Q}$, and is the norm of $\mathfrak{Q}$ in the sense of divisors. π maps paths $\mathfrak{B}$ on $R(K)$ into paths $\pi\mathfrak{B}$ on $R(k)$. Applied to closed paths through a fixed base point $\mathfrak{O}$ on $R(K)$, this map induces a monomorphism of the fundamental group $F(K)$ of $R(K)$ (based on $\mathfrak{O}$) into the fundamental group $F(k)$ of $R(k)$ (based on $o = \pi\mathfrak{O}$). K/k is normal if and ony if $\pi F(K)$ is a normal subgroup of $F(k)$, in which case $G(K/k) \approx F(k)/\pi F(K)$.

There is also a map of 1-cells on the ground surface $R(k)$ into 1-chains on the covering surface $R(K)$, which we call the transfer map and denote by V. If γ is a 1-cell on $R(k)$, then V_γ is the sum of all the 1-cells on $R(K)$ which lie over γ. More precisely, if γ has beginning point $\mathfrak{o}$, and if $\mathfrak{O}_j$, $1 \leqq j \leqq n = [K:k]$, are the points above $\mathfrak{o}$, then for each j there is a unique path Γ_j on $R(K)$ which begins at $\mathfrak{O}_j$ and cover γ; we put $V_\gamma = \sum_{j=1}^{n} \Gamma_j$. Obviously the existence of this map V depends on the finiteness of the covering. V carries cycles into cycles, and induces a homomorphism $V: H_1(k) \to H_1(K)$. If we identitfy H_1 with the factor commutator group F/F', and view $F(K)$ as subgroup of $F(k)$ by the imbedding π, then it is easy to see that this homomorphism V is none other than the group theoretical transfer or *Verlagerung* from $F(k)$ into the subgroup $F(K)$.

We define the trace map S of differentials of K into those of k, and the cotrace map S^* in the opposite direction by the formulas

$$(27) \qquad (SdU)(\mathfrak{q}) = \sum_{\mathfrak{Q}|\mathfrak{q}} dU(\mathfrak{Q}), \qquad (S^*du)(\mathfrak{Q}) = du(\pi\mathfrak{Q}).$$

From these definitions, the rules

$$(28) \qquad \int_\gamma SdU = \int_{V_\gamma} dU, \qquad \int_\Gamma S^*du = \int_{\pi\Gamma} du,$$

are evident. Concerning our special differentials of the third kind we have

$$(29) \qquad Sd\log\mathfrak{A} = d\log N\mathfrak{A}. \qquad S^*d\log\mathfrak{a} = d\log i\mathfrak{a},$$

where N is the norm map of ideals from K to k and i is the injection map of ideals of k into K. To prove (29) one has simply to observe that the left hand sides have the characterizing properties of the right. Indeed, from (28) we see that the left hand sides have pure imaginary periods, and from the definition of S and S^* it is easily checked that they have the correct residues. Combining (28) and (29) we obtain the following rules for our symbol:

$$(30) \qquad (\beta, N\mathfrak{A})_k = (V\beta, \mathfrak{A})_K; \qquad (\mathrm{B}, i\mathfrak{a})_K = (\pi\mathrm{B}, \mathfrak{a})_k.$$

Choosing a point $\mathfrak{P} \varepsilon R(K)$ with which to describe the characters $\chi_K(\Gamma, \lambda)$ of K, and using $\mathfrak{p} = \pi\mathfrak{P}$ to describe the characters $\chi_k(\gamma, \lambda)$ of k, we find the following formulas for the conorm and norm of characters:

$$(31) \qquad N^*(\chi_k(\gamma, \lambda)) = \chi_K(V_\gamma, \lambda),$$

$$(32) \qquad N(\chi_K(\Gamma, \lambda)) = \chi_k(\pi\Gamma, \lambda^n(\Gamma, \mathfrak{p}\mathfrak{P}^{-n})_K),$$

where $n = [K:k]$. Indeed, from (30), it follows that the left sides give the same values as the right sides when applied to divisors of degree 0, and one can easily check directly that they give the same when applid to $\mathfrak{P}$, resp. $\mathfrak{p}$. Since the map $\lambda \to \lambda^n$ maps T onto T, (32) shows that the character norm group $N(\hat{E}(K))$ is equal to $\chi_k(\pi H_1(K), T)$, and consequently,

$$\hat{E}(k)/N\hat{E}(K) \approx H_1(k)/\pi H_1(K). \tag{33}$$

If K/k is abelian with group G, then the correspondence which attaches to each element of $H_1(k)$ the corresponding covering transformation of $R(K)$ induces an isomorphism

$$H_1(k)/\pi H_1(K) \approx G. \tag{34}$$

(Covering transformations can be associated with homology classes rather than homotopy classes because the covering is assumed abelian.) We contend that the reciprocity law isomorphism of our pseudo class field theory is obtained by combining the isomorphisms (33) and (34). To prove this, we let $\chi_{\sigma,\tau} = \chi_K(\Gamma_{\sigma,\tau}, \lambda_{\sigma,\tau})$ be a fundamental 2-cocycle for K/k of the type described a few paragraphs above, and we compute the Nakayama map associated with χ. This is the map

$$\rho \to \prod_\sigma \chi_{\sigma,\rho} = \prod_\sigma \chi_K(\Gamma_{\sigma,\rho}, \lambda_{\sigma,\rho}) = \chi_K(\sum_\sigma \Gamma_{\sigma,\rho}, \prod_\sigma \lambda_{\sigma,\rho}).$$

To work this out we use the definition of $\Gamma_{\sigma,\rho}$ and find

$$\sum_\sigma \Gamma_{\sigma,\rho} = \sum_\sigma (\mathrm{B}_\sigma - \mathrm{B}_{\sigma\rho} + \sigma \mathrm{B}_\rho) = \sum_\sigma \sigma \mathrm{B}_\rho = V\beta_\rho,$$

where $\beta_\rho = \pi \mathrm{B}_\rho$, the paths $\sigma \mathrm{B}_\rho$, $\sigma \in G$, being then just those paths on $R(K)$ above β_ρ. Combining these last two computations and using (31) we find

$$\prod_\sigma \chi_{\sigma,\rho} = \chi_K(V\beta_\rho, \prod_\sigma \lambda_{\sigma,\rho}) = N^* \chi_k(\beta_\rho, \lambda_\rho),$$

where $\lambda_\rho = \prod_\sigma \lambda_{\sigma,\rho}$. According to the explicit formula (I, 22) of the first half of this paper, we conclude that the reciprocity law attaches the automorphism ρ to the coset of $\chi_k(\beta_\rho, \lambda_\rho) \bmod N\hat{E}(K)$. To prove our contention therefore, we have only to show that ρ is the covering transformation attached to β_ρ. But that is obvious because $\beta_\rho = \pi \mathrm{B}_\rho$, and B_ρ was a path on $R(K)$ leading from the base point $\mathfrak{O}$ to $\mathfrak{O}^\rho$.

Weil [8] has remarked that the kernel of this infinite reciprocity law map of ordinary class field theory is the connected component of the idèle class group. The same is true for our pseudo class field theory. Viewing

$H_1(k)$ as an everywhere dense subgroup of the Galois group $G(A_k/k)$ of the (infinite) maximal abelian extension A_k of k, we see from what we have just proved, that the infinite reciprocity law map is just the natural map $\hat{E}(k) \to H_1(k)$. Its kernel is isomorphic to T, and is evidently the connected component of $\hat{E}$.

INSTITUTE FOR ADVANCED STUDY,
PRINCETON UNIVERSITY.

REFERENCES.

[1] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton University Press (forthcoming).

[2] H. Weyl, *Die Idee der Riemannschen Fläche*, Teubner, Leipzig, 1923.

[3] J. Igusa, "Zur klassischen Theorie der algebraischen Functionen," *Journal of the Mathematical Society of Japan*, vol. 1 (1943), pp. 63-72.

[4] E. Artin, *Algebraic Numbers and Alegbraic Functions I*, Mimeographed Notes, New York University, 1951.

[5] G. Hochschild and T. Nakayama, "Cohomology in class field theory," *Annals of Mathematics*, vol. 55 (1952), pp. 348-366.

[6] J. Tate, "The higher dimensional cohomology groups of class field theory," *ibid.*, vol. 56 (1952), pp. 294-297.

[7] E. Artin and J. Tate, *Algebraic Numbers and Algebraic Functions II*, Mimeographed Notes, New York University (in preparation).

[8] A. Weil, "Sur la théorie du corps de classes," *Journal of the Mathematical Society of Japan*, vol. 3 (1951), pp. 1-35.

[9] C. Chevalley, *Class Field Theory*, Nagoya University, Japan, 1954.

LIE GROUPS AND LIE HYPERALGEBRAS OVER A FIELD OF CHARACTERISTIC $p > 0$ (II).*

By JEAN DIEUDONNÉ.

---

1. Introduction. This paper is a continuation of two earlier ones ([3], [5]); we keep the same notations and terminology. We first complete the general theory outlined in these papers by giving characterizations of a Lie hyperalgebra and of a derived homomorphism; unfortunately, these characterizations do not seem at present to provide very useful tools for further development of the theory. In the remainder of the paper, we first study the formal Lie groups of *dimension one* over an algebraically closed field; we are able to characterize, among those groups, those which are isomorphic to the multiplicative group W_1*, by the consideration of its Lie *algebra* only; moreover, we can show that the hyperalgebras of all *abelian* Lie groups of dimension one can be reduced to well determined types, forming a denumerable sequence; but the question remains open of the existence of groups corresponding to each of these hyperalgebras.[1] Finally, the same methods yield some information on general abelian formal Lie groups, but (even when the base field is algebraically closed) the complete description of these groups still seems a problem of considerable difficulty.

2. General results. Let G be a formal Lie group of dimension n over a field K of characteristic $p > 0$. In the "Taylor formula" for G ([3], formulas (25) and (28)),

$$f(xy) = \sum_{\alpha} P_\alpha(y) X_\alpha f \tag{1}$$

---

* Received November 6, 1954.

[1] Since this paper was written, M. Lazard has proved that every one-dimensional formal Lie group is necessarily abelian (C. R. Acad. Sci. Paris, vol. 239 (1954), pp. 942-945). On the other hand, I have proved the existence of all one-dimensional abelian Lie groups whose hyperalgebras are described in Theorem 2 (no. 8); the proof will be published in a forthcoming paper in *Mathematische Zeitschrift*.

Added in proof. In a paper to appear in *Bull. Soc. Math. France*, M. Lazard has independently obtained the classification and existence of one-dimensional formal Lie groups over an algebraically closed field, by an entirely different method.

we can rearrange the series in the right-hand member by grouping the terms containing the same monomial y_α in $\mathbf{y}$, and write [2]

$$f(\mathbf{xy}) = \sum_\alpha y_\alpha Z_\alpha f. \tag{2}$$

From the properties of the series P_α ([3], no. 10), it follows that Z_α is a finite combination of invariant differential operators X_λ of height $h(\lambda) \leqq h(\alpha)$, which can also be characterized as those satisfying the "initial conditions" $Z_\alpha(\mathbf{e}) = (1/\alpha!) D_\alpha(\mathbf{e})$ for every α, and therefore are obviously linearly independent over the ring $\mathfrak{o}$ of formal power series. The arguments used in [3, no. 11] can then be repeated *verbatim* for x_α and Z_α instead of $P_\alpha(\mathbf{x})$ and X_α; in particular, if we write

$$Z_\alpha Z_\beta = \sum_\gamma d_{\alpha\beta\gamma} Z_\gamma \tag{3}$$

(with the convention $Z_0 = I$, hence $d_{\alpha 0\beta} = d_{0\alpha\beta} = \delta_{\alpha\beta}$ and $d_{\alpha\beta 0} = 0$ if $\alpha \neq 0$ or $\beta \neq 0$), we have

$$Z_\beta x_\alpha = \sum_\gamma d_{\gamma\beta\alpha} x_\gamma \tag{4}$$

and moreover, the group law is expressed by the series

$$\phi_i(\mathbf{x}, \mathbf{y}) = \sum_{\alpha,\beta} d_{\alpha\beta\epsilon_i} x_\alpha y_\beta \qquad (1 \leqq i \leqq n) \tag{5}$$

where $\epsilon_i = (0, \cdots, 0, 1, 0, \cdots, 0)$, with 1 at the i-th place.

In addition to these relations, we note that if $h = fg$ is a product of two power series, $h(\mathbf{xy}) = f(\mathbf{xy}) g(\mathbf{xy})$. Let us (partially) order the set of indices $\alpha = (\alpha_1, \cdots, \alpha_n)$ in the usual way, writing $(\alpha_1, \cdots, \alpha_n) \leqq (\beta_1, \cdots, \beta_n)$ to mean $\alpha_i \leqq \beta_i$ for each i. Then, the preceding relation and the "Taylor formula" (2) yield immediately for the operators Z_α, the "generalized Leibniz formula"

$$Z_\alpha(fg) = \sum_{0 \leqq \beta \leqq \alpha} (Z_\beta f)(Z_{\alpha-\beta} g). \tag{6}$$

Conversely:

PROPOSITION 1. *For each α, let Z_α be a K-linear endomorphism of $\mathfrak{o}$ such that $Z_0 = I$ and that each Z_α is a special semi-derivation of height $h(\alpha) + 1$; and suppose these operators verify the relations* (3), (4) *and* (6), *with $d_{\alpha 0\beta} = d_{0\alpha\beta} = \delta_{\alpha\beta}$. Then formulae* (5) *define a group law, for which* (2) *is the Taylor formula.*

From the assumption that the Z_α are semi-derivations, it follows that if $f(\mathbf{x}) = \sum_\lambda a_\lambda x_\lambda$, we can write $Z_\alpha f(\mathbf{x}) = \sum_\lambda a_\lambda Z_\alpha x_\lambda$, by expressing f as a

[2] The idea to work systematically with the Z_α instead of the X_α occurred to me during several stimulating talks I had with J. Delsarte on this and related topics.

polynomial with coefficients in an $\mathfrak{o}_r$, with $r > h(\alpha)$. Let us define the operator R_y on $\mathfrak{o}$ by the equation

$$R_y f(x) = \sum_\alpha y_\alpha Z_\alpha f(x). \tag{7}$$

It follows from (6) that $R_y(fg) = (R_y f)(R_y g)$; on the other hand, one can write $R_y f(x) = \sum_\lambda a_\lambda R_y(x_\lambda)$; but

$$R_y(x_\lambda) = (R_y(x_1))^{\lambda_1} \cdot \cdots \cdot (R_y(x_n))^{\lambda_n}$$

and from (4) it follows that $\phi_i(x, y) = R_y(x_i)$ is given by formula (5) $(1 \leqq i \leqq n)$. We can therefore write

$$R_y f(x) = f(\phi_1(x, y), \cdots, \phi_n(x, y)). \tag{8}$$

It follows from (7) that $R_e f(x) = f(x)$; on the other hand, the relations (4) and $d_{0\alpha\beta} = \delta_{\alpha\beta}$ show that the value of $Z_\beta x_\alpha$ for $x = e$ is $\delta_{\alpha\beta}$; hence $Z_\alpha f(e) = a_\alpha$, and therefore $R_y f(e) = f(y)$; in particular $\phi_i(e, x) = \phi_i(x, e) = x_i$. On the other hand, let us write $L_y f(x) = R_x f(y)$; this is again a linear operator on $\mathfrak{o}$, and the associativity conditions are equivalent to the commutativity relation

$$R_y L_z = L_z R_y. \tag{9}$$

To prove (9), we notice that

$$\begin{aligned} R_y L_z f(x) &= \sum_{\alpha,\beta} y_\alpha (Z_\alpha x_\beta)(Z_\beta f(z)) \\ &= \sum_{\alpha,\beta,\gamma} d_{\gamma\alpha\beta} x_\gamma y_\alpha (Z_\beta f(z)) \end{aligned}$$

due to (4); on the other hand, (3) shows that

$$\begin{aligned} L_z R_y f(x) &= \sum_{\alpha,\beta} x_\alpha y_\beta (Z_\alpha Z_\beta f(z)) \\ &= \sum_{\alpha,\beta,\gamma} d_{\alpha\beta\gamma} x_\alpha y_\beta (Z_\gamma f(z)) \end{aligned}$$

whence (9), and this ends our proof.

It is easy to verify that the definition (4) of the linear operators Z_α, together with the associativity conditions

$$\sum_\lambda d_{\alpha\beta\lambda} d_{\lambda\gamma\delta} = \sum_\lambda d_{\beta\gamma\lambda} d_{\alpha\lambda\delta} \tag{10}$$

for the coefficients, imply the "multiplication table" (3). On the other hand, relations (6) are equivalent to the relations obtained by applying them to $f = x_\lambda$, $g = x_\mu$, that is

$$d_{\alpha,\beta,\lambda+\mu} = \sum_{\substack{0 \leqq \gamma \leqq \alpha \\ 0 \leqq \delta \leqq \beta}} d_{\gamma\delta\lambda} d_{\alpha-\gamma,\beta-\delta,\mu} \tag{11}$$

for all indices $\alpha, \beta, \lambda, \mu$. A Lie hyperalgebra may thus be said to consist in a family $(d_{\alpha\beta\gamma})$ of elements of K satisfying (10) and (11), and such that $d_{0\alpha\beta} = d_{\alpha 0\beta} = \delta_{\alpha\beta}$, $d_{\alpha\beta 0} = 0$ except for $\alpha = \beta = 0$, $d_{000} = 1$, and $d_{\alpha\beta\gamma} = 0$ if $x_\gamma \in \mathfrak{o}_r$, and $r > h(\gamma)$; but it is obvious that such a description is hardly a workable one.

3. Let now $\boldsymbol{u}$ be a homomorphism of G into a formal Lie group $\bar{G}$ of dimension m; the arguments of [3, no. 12] can be applied to the x_α and Z_α and show that one can write

$$\boldsymbol{u}'(Z_\alpha) = \sum_\lambda a_{\alpha\lambda} \bar{Z}_\lambda \tag{12}$$

and

$$\bar{f}(\boldsymbol{u}(\boldsymbol{x})) = \sum_\alpha x_\alpha (\boldsymbol{u}'(Z_\alpha)(\bar{\boldsymbol{e}}))\bar{f} = \sum_\lambda (\boldsymbol{u}(\boldsymbol{x}))_\lambda \bar{Z}_\lambda(\bar{\boldsymbol{e}})\bar{f} \tag{13}$$

where $(\boldsymbol{u}(\boldsymbol{x}))_\lambda$ means $\bar{x}_\lambda$ in which $u_i(\boldsymbol{x})$ has been substituted for $\bar{x}_i$ $(1 \leqq i \leqq m)$. In addition, if $\bar{h} = \bar{f}\bar{g}$, one has $\bar{h}(\boldsymbol{u}(\boldsymbol{x})) = \bar{f}(\boldsymbol{u}(\boldsymbol{x}))\bar{g}(\boldsymbol{u}(\boldsymbol{x}))$ and therefore formula (13) yields the conditions

$$\boldsymbol{u}'(Z_\alpha)(\bar{f}\bar{g}) = \textstyle\sum_{0 \leqq \beta \leqq \alpha} (\boldsymbol{u}'(Z_\beta)(\bar{f}))(\boldsymbol{u}'(Z_{\alpha-\beta})(\bar{g})). \tag{14}$$

Conversely:

PROPOSITION 2. *Let $\boldsymbol{u}'$ be a homomorphism of the Lie hyperalgebra of G into that of $\bar{G}$ satisfying conditions* (14), *transforming the unit element into the unit element and sending each $\mathfrak{g}_r$ into $\bar{\mathfrak{g}}_r$. Then $\boldsymbol{u}'$ is the derived homomorphism of a homomorphism $\boldsymbol{u}$ of G into $\bar{G}$.*

Let us define a mapping C of $\mathfrak{o}(\bar{G})$ into $\mathfrak{o}(G)$ by the formula

$$C\bar{f} = \sum_\alpha x_\alpha (\boldsymbol{u}'(Z_\alpha)(\dot{\boldsymbol{e}}))\bar{f}; \tag{15}$$

it follows from (14) that $C(\bar{f}\bar{g}) = C(\bar{f})C(\bar{g})$, in other words C is a ring homomorphism. If $\boldsymbol{u}'(Z_\alpha)$ is given by (12), let us define

$$u_i(\boldsymbol{x}) = C(\bar{x}_i) = \sum_\alpha a_{\alpha\varepsilon_i} x_\alpha \text{ for } 1 \leqq i \leqq m. \tag{16}$$

Then, from (15) and (12) it follows that

$$C(\bar{x}_\lambda) = (u_1(\boldsymbol{x}))^{\lambda_1} \cdots (u_m(\boldsymbol{x}))^{\lambda_m} = \sum_\alpha a_{\alpha\lambda} x_\alpha. \tag{17}$$

Formula (15) and the assumption that $\boldsymbol{u}'$ sends $\mathfrak{g}_r$ into $\bar{\mathfrak{g}}_r$ for each r imply that C transforms $\mathfrak{o}_r(\bar{G})$ into a subring of $\mathfrak{o}_r(G)$. If we write the Taylor formula in $\bar{G}$

$$\bar{f}(\bar{\boldsymbol{x}}) = \sum_\lambda \bar{x}_\lambda \bar{Z}_\lambda(\bar{\boldsymbol{e}})\bar{f}$$

we deduce from the preceding remarks that one has

$$C\check{f} = \sum_{\lambda} C(\bar{x}_\lambda)\bar{Z}_\lambda(\bar{e})\check{f} = \check{f}(\boldsymbol{u}(\boldsymbol{x})).$$

To prove that $\boldsymbol{u}$ is a homomorphism of G into $\bar{G}$, we have to prove the relation

$$CR_{\boldsymbol{u}(\boldsymbol{y})} = R_{\boldsymbol{y}}C. \tag{18}$$

But one has

$$R_{\boldsymbol{u}(\boldsymbol{y})}\check{f} = \sum_{\lambda,\mu} \bar{x}_\lambda(\boldsymbol{u}(\boldsymbol{y}))_\mu(\bar{Z}_\lambda\bar{Z}_\mu(\bar{e}))\check{f}$$

hence

$$CR_{\boldsymbol{u}(\boldsymbol{y})}\check{f} = \sum_{\lambda,\mu} (\boldsymbol{u}(\boldsymbol{x}))_\lambda(\boldsymbol{u}(\boldsymbol{y}))_\mu(\bar{Z}_\lambda\bar{Z}_\mu(\bar{e}))\check{f}.$$

Therefore, (17) and the assumption that $\boldsymbol{u}'$ is a homomorphism enable one to write

$$\begin{aligned} CR_{\boldsymbol{u}(\boldsymbol{y})}\check{f} &= \sum_{\alpha,\beta} x_\alpha y_\beta(\boldsymbol{u}'(Z_\alpha Z_\beta)(\bar{e}))\check{f} \\ &= \sum_{\alpha,\beta,\gamma} d_{\alpha\beta\gamma}x_\alpha y_\beta(\boldsymbol{u}'(Z_\gamma)(\bar{e}))\check{f} \end{aligned}$$

and, using (4)

$$CR_{\boldsymbol{u}(\boldsymbol{y})}\check{f} = \sum_{\beta,\gamma} y_\beta(Z_\beta x_\gamma)(\boldsymbol{u}'(Z_\gamma)(\bar{e}))\check{f};$$

but, from (15), this is also

$$\sum_{\beta} y_\beta(Z_\beta C\check{f}) = R_{\boldsymbol{y}}C\check{f}$$

using formula (7), and this ends the proof.

4. In what follows, we will use repeatedly the notion of *canonical group law*; we will give here a brief summary of the definitions and results pertaining to this notion (for the proofs, see [5]). To say that the group law of G is canonical means that the power series $P_{0i}(\boldsymbol{x}) = x_i$ for $1 \leqq i \leqq n$; from (2), it follows that this is equivalent to the following property of the Z_α: *if α is distinct from ϵ_i $(1 \leqq i \leqq n)$, the coefficient of each X_{0j} $(1 \leqq j \leqq n)$ in the expression of Z_α as linear combination of the X_λ is* 0.

When the group law of G is not canonical, there exists an isomorphism $\boldsymbol{u}$ of G onto a group $\bar{G}$ having canonical law. Such an isomorphism can be obtained by a "standard process" described in detail in [5]: one considers an infinite sequence $(G^{(r)})$ of groups, with $G^{(0)} = G$, and for each r one defines an isomorphism $\boldsymbol{u}^{(r)}$ of $G^{(r)}$ onto $G^{(r+1)}$ by the formulae $u_i^{(r)}(\boldsymbol{x}) = P_{0i}^{(r)}(\boldsymbol{x})$ for $1 \leqq i \leqq n$; it turns out that $u_i^{(r)}(\boldsymbol{x}) = x_i + v_i^{(r)}(\boldsymbol{x})$ where the monomials in $v_i^{(r)}$ have all a height $\geqq r$, and moreover there are no monomials of type $x_j^{p^k}$ for $k \geqq 1$ (see [3, formula (34)]). The group $\bar{G}$ with canonical law and

the isomorphism $\boldsymbol{u}$ are obtained by a "passage to the limit" from $G^{(r)}$ and the composite isomorphism $\boldsymbol{u}^{(r)}\boldsymbol{u}^{(r-1)} \cdot \cdot \cdot \boldsymbol{u}^{(0)}$.

The importance of the notion of canonical law lies chiefly in the *uniqueness theorem* [5, Th. 2] which can be stated in the slightly more general following form (following from the proof of Theorem 2 in [5]): *if the group laws of two n-dimensional formal Lie groups G, H are canonical, and if the constants $c_{\alpha\beta\gamma}$ which determine the multiplication of the X_α in the hyperalgebras of G and H* (see [3, no. 11]) *are the same in both groups for $h(\alpha) < r$, $h(\beta) < r$* (and necessarily $h(\gamma) < r$) *then the constants $d_{\alpha\beta\gamma}$* (see formula (3)) *are also the same in G and H for $h(\alpha) < r$ and $h(\beta) < r$.*

Finally, we prove the following

PROPOSITION 3. *If the group law is canonical, one has $Z_\alpha = (1/\alpha!)X_\alpha$ for all indices α of height $h(\alpha) = 0$.*

We will use induction on the total degree $|\alpha|$, the proposition being obvious for $|\alpha| = 1$. Let $\alpha = (0, \cdot \cdot \cdot, 0, \alpha_i, \alpha_{i+1}, \cdot \cdot \cdot, \alpha_n)$, α_i being the first component $\neq 0$; we can therefore write $\alpha = \alpha_i\epsilon_i + \beta$, where $\beta = (0, \cdot \cdot \cdot, 0, \alpha_{i+1}, \cdot \cdot \cdot, \alpha_n)$. The proposition will be proved if we establish that the difference $Z_\alpha - \frac{1}{\alpha!}X_\alpha$ is a *derivation*; for it will then have to be a linear combination of the X_{0j} $(1 \leqq j \leqq n)$, and if $|\alpha| > 1$, this linear combination must reduce to 0, due to the assumption that the group law is canonical.

Now we have, from (6) and the induction hypothesis

$$Z_\alpha(fg) = f \cdot Z_\alpha g + g \cdot Z_\alpha f + \sum_{(\lambda_i,\gamma)} \left(\frac{1}{\lambda_i!}X_{0i}^{\lambda_i}Z_\gamma f\right)\left(\frac{1}{(\alpha_i - \lambda_i)!}X_{0i}^{\alpha_i-\lambda_i}Z_{\beta-\gamma}g\right)$$

where in the summation, the pair (λ_i, γ) ranges over the set satisfying the conditions $0 \leqq \lambda_i \leqq \alpha_i$ and $0 \leqq \gamma \leqq \beta$, with the exception of the two pairs $(0, 0)$ and (α_i, β). On the other hand, we have similarly

$$\frac{1}{\alpha!}X_\alpha = \frac{1}{\alpha_i}X_{0i}Z_{\alpha-\epsilon_i}$$

and

$$Z_{\alpha-\epsilon_i}(fg) = \sum_{(\mu_i,\gamma)} \left(\frac{1}{\mu_i!}X_{0i}^{\mu_i}Z_\gamma f\right)\left(\frac{1}{(\alpha_i - \mu_i - 1)!}X_{0i}^{\alpha_i-\mu_i-1}Z_{\beta-\gamma}g\right)$$

where in the summation, $0 \leqq \mu_i \leqq \alpha_i - 1$, $0 \leqq \gamma \leqq \beta$; therefore

$$\frac{1}{\alpha!}X_\alpha(fg) = \frac{1}{\alpha_i}\sum_{(\mu_i,\gamma)} \left(\left(\frac{1}{\mu_i!}X_{0i}^{\mu_i+1}Z_\gamma f\right)\left(\frac{1}{(\alpha_i - \mu_i - 1)!}X_{0i}^{\alpha_i-\mu_i-1}Z_{\beta\ \gamma}g\right)\right.$$
$$\left. + \left(\frac{1}{\mu_i!}X_{0i}^{\mu_i}Z_\gamma f\right)\left(\frac{1}{(\alpha_i - \mu_i - 1)!}X_{0i}^{\alpha_i-\mu_i}Z_{\beta-\gamma}g\right)\right)$$

with the same range in the summation. As

$$\frac{1}{\alpha_i}\left(\frac{1}{\mu_i!(\alpha_i-\mu_i-1)!}+\frac{1}{(\mu_i-1)!(\alpha_i-\mu_i)!}\right)=\frac{1}{\mu_i!(\alpha_i-\mu_i)!}$$

we have

$$Z_\alpha(fg)-\frac{1}{\alpha!}X_\alpha(fg)=f(Z_\alpha g-\frac{1}{\alpha!}X_\alpha g)+g(Z_\alpha f-\frac{1}{\alpha!}X_\alpha f)$$

and the proof is complete.

This result corresponds of course to the "exponential" expression of the Taylor formula in canonical coordinates, in the classical case; but examples show that there is no such "universal" expression of Z_α as a polynomial in the X_λ, which would be valid for *every* canonical group law, when $h(\alpha)>1$.

5. One-dimensional groups. We first prove two lemmas which will be used repeatedly later on.

LEMMA 1. *Suppose Z_λ and Z_μ are permutable for the pairs (λ,μ) such that, either $0\leqq\lambda\leqq\alpha$, $0\leqq\mu<\beta$, or $0\leqq\lambda<\alpha$, $0\leqq\mu\leqq\beta$; then $[Z_\alpha, Z_\beta]$ is a derivation.*

Indeed, it follows from (6) that

$$Z_\alpha Z_\beta(fg)=\sum_{\substack{0\leqq\lambda\leqq\alpha\\0\leqq\mu\leqq\beta}}(Z_\lambda Z_\mu f)\,(Z_{\alpha-\lambda}Z_{\beta-\mu}g)$$

and

$$Z_\beta Z_\alpha(fg)=\sum_{\substack{0\leqq\lambda\leqq\alpha\\0\leqq\mu\leqq\beta}}(Z_\mu Z_\lambda f)\,(Z_{\beta-\mu}Z_{\alpha-\lambda}g)$$

But, in the range of summation, one has $Z_\lambda Z_\mu=Z_\mu Z_\lambda$ except for the pair $\lambda=\alpha$, $\mu=\beta$; hence

$$(Z_\alpha Z_\beta-Z_\beta Z_\alpha)(fg)=f\cdot(Z_\alpha Z_\beta-Z_\beta Z_\alpha)g+g\cdot(Z_\alpha Z_\beta-Z_\beta Z_\alpha)f$$

which ends the proof.

LEMMA 2. *Suppose the Z_λ corresponding to the range $0\leqq\lambda\leqq\alpha$ are mutually permutable; then*

$$Z_\alpha{}^p(fg)=\sum_{0\leqq\lambda\leqq\alpha}(Z_\lambda{}^p f)\,(Z_{\alpha-\lambda}{}^p g). \tag{19}$$

It will be enough to prove that, for every integer m, one has

$$Z_\alpha{}^m(fg)=\left(\sum_{0\leqq\lambda\leqq\alpha}(Z_\lambda f)\,(Z_{\alpha-\lambda}g)\right)^{(m)}$$

where, in the "symbolic power", a product $(Z_{\lambda_1}f)\,(Z_{\lambda_2}f)\cdots(Z_{\lambda_k}f)$ has to be replaced by $(Z_{\lambda_1}Z_{\lambda_2}\cdots Z_{\lambda_k})f$, and similarly for the products of $Z_\mu g$; by

induction on m, this follows immediately from (6) and the assumption that all the Z_λ which intervene commute.

6. From now on until **12**, we shall suppose that the field K is *algebraically closed.* For a one-dimensional group G, we shall write X_h instead of X_{h1}; we have therefore $X_0^p = aX_0$; if $a \neq 0$, the change of variable $\bar{x}_1 = u(x_1) = \lambda x_1$ is such that $u'(X_0) = \lambda \bar{X}_0$, hence $u'(X_0^p) = \lambda^p \bar{X}_0^p = a\lambda \bar{X}_0$. It is therefore possible to choose $\lambda \in K$ such that one is reduced to the case $a = 1$.

Case A. $X_0^p = X_0$. We may suppose [5] that the group law of G is *canonical.* Our first goal is to prove that X_1 and X_0 commute; from Prop. 3 it follows that Lemma 1 can be applied to the indices 1 and p, and therefore

$$X_1X_0 - X_0X_1 = cX_0 \tag{20}$$

is a derivation; by induction on k, we get

$$X_1X_0^p - X_0^kX_1X_0^{p-k} = kcX_0 \tag{21}$$

and in particular, for $k = p$

$$X_1X_0^p - X_0^pX_1 = 0. \tag{22}$$

Comparing (20) and (22) and using the assumption $X_0^p = X_0$ yields $c = 0$.

7. We shall now define an inductive process which will ultimately give us the structure of G.

We start from a one-dimensional group $G^{(r)}$, with canonical group law, and we suppose that: 1. $X_0^{(r)}, X_1^{(r)}, \cdots, X_{r-1}^{(r)}$ *are mutually permutable*; 2. $(X_h^{(r)})^p = X_h^{(r)}$ *for* $0 \leqq h \leqq r-1$. We want to define an isomorphism $v^{(r)}$ of $G^{(r)}$ on a similar group $G^{(r+1)}$, such that $v^{(r)}(x^{(r)}) = x^{(r)} + \mu(x^{(r)})^{p^r} + \cdots$ (terms omitted of degree $> p^r$).

For convenience, we drop the upper index r, and speak therefore of G instead of $G^{(r)}$. We first observe that, as the Z_α for $\alpha < p^r$ are polynomials in $X_0, \cdots, X_{r-1}$, they are mutually permutable. Lemma 1 may therefore be applied, first to X_0 and X_r, which gives

$$X_rX_0 - X_0X_r = b_0X_0 \tag{23}$$

and the same argument as in **6** shows that $b_0 = 0$. Suppose we have proved that X_r commutes with $X_0, X_1, \cdots, X_{k-1}$; as the Z_α for $\alpha < p^k$ are poly-

nomials in $X_0, \cdots, X_{k-1}$, they commute with X_r; Lemma 1 may again be applied to X_k and X_r, which gives

$$X_r X_k - X_k X_r = b_k X_0. \tag{24}$$

We treat this equation in the same way as (20), writing first

$$X_r X_k^p - X_k X_r X_k^{p-1} = b_k X_0 X_k^{p-1}.$$

By induction on h, and using the fact that X_0 and X_k commute, we get

$$X_r X_k^p - X_k^h X_r X_k^{p-h} = h b_k X_0 X_k^{p-1} \qquad (1 \leqq h \leqq p) \tag{25}$$

and in particular, for $h = p$, and using the relation $X_k^p = X_k$, we see that X_k and X_r commute. We have thus shown that X_r commutes with X_k for $0 \leqq k \leqq r-1$.

The next step consists first in remarking that $Z_\alpha^p = Z_\alpha$ for $\alpha \leqq p^r - 1$. This is clear by assumption for $\alpha = 1, p, \cdots, p^{r-1}$; it is proved by induction on α for the other values of α. Indeed, we have, by Lemma 2 and the induction hypothesis

$$Z_\alpha^p(fg) = f \cdot Z_\alpha^p g + g \cdot Z_\alpha^p f + \sum_{1 \leqq \lambda \leqq \alpha-1} (Z_\lambda f)(Z_{\alpha-\lambda} g) \tag{26}$$

from which one deduces immediately that $Z_\alpha^p - Z_\alpha$ is a *derivation*. But in the expression of Z_α as a linear combination of the X_λ ($\lambda \leqq \alpha$), there is no term in X_0 (from the assumption that the group law is canonical); as $X_k^p = X_k$ for every $k < r$ (from the inductive assumption), we have necessarily $Z_\alpha^p - Z_\alpha = 0$. This result being obtained, we can apply Lemma 2 to $\alpha = p^r$, since X_r commutes with the Z_α of index $\alpha < p^r$; we obtain

$$X_r^p(fg) = f \cdot X_r^p g + g \cdot X_r^p f + \sum_{1 \leqq \lambda \leqq p^r} (Z_\lambda f)(Z_{p^r-\lambda} g)$$

and therefore $X_r^p - X_r$ is a *derivation*, in other words

$$X_r^p - X_r = b X_0. \tag{27}$$

We now consider the transformation $v_1(x) = x + \lambda x^{p^r}$; this is an isomorphism of G on a group G_1, and formulae (12) and (17) show that

$$\begin{cases} v'_1(X_k) = X_k^{(1)} & \text{for} \quad 0 \leqq k \leqq r-1 \\ v'_1(X_r) = X_r^{(1)} + \lambda X_0^{(1)}. \end{cases} \tag{28}$$

Equation (27) yields therefore

$$(X_r^{(1)})^p - X_r^{(1)} = (b + \lambda - \lambda^p) X_0^{(1)}$$

and it is possible to choose λ such that the right-hand side vanishes. The group law of G_1 is not perhaps a canonical one; but from formula (13) and

the definition of v_1, it follows at once that for $\alpha < p^r$, $v'_1(Z_\alpha) = Z_\alpha^{(1)}$; formulae (28) prove therefore that the expression of $Z_\alpha^{(1)}$ for $\alpha < p^r$, as linear combination of the $X_\lambda^{(1)}$, has the same coefficients as those in the expression of Z_α as combination of the X_λ. The first $Z_\alpha^{(1)}$ which may contain X_0 are therefore of degree $\alpha > p^r$, in other words, one has

$$P^{(1)}(x^{(1)}) = x^{(1)} + a(x^{(1)})^{p^{r+1}} + \cdots. \tag{29}$$

The standard method, which yields a canonical group law from an arbitrary one (see **4**), shows then that there exists an isomorphism v_2 of G_1 onto a group $\bar{G}$ with canonical group law, such that $v'_2(X_k^{(1)}) = \bar{X}_k$ for $0 \leqq k \leqq r$, and in addition the isomorphism $v = v_2 v_1$ of G on $\bar{G}$ has the form $v(x) = x + \lambda x^{p^r} + \cdots$.

Returning to our original notations, we have therefore proved the existence of the isomorphism $v^{(r)}$. Starting now from $G = G^{(0)}$, we consider the isomorphism $u^{(r)} = v^{(r)} v^{(r-1)} \cdots v^{(0)}$ of G on $G^{(r+1)}$. It is clear that, in the formal power series $u^{(r)}(x)$, the terms of degree $< p^m$ are *the same* for all $r > m$; we can therefore define a power series u by the condition that all terms of u of degree $< p^m$ are those of every series $u^{(r)}$ for $r > m$. It follows that $w^{(r)} = u(u^{(r)})^{-1}$ is an isomorphism of $G^{(r)}$ on a group $\bar{G}$, such that $w^{(r)}(x^{(r)}) = x^{(r)} + \lambda(x^{(r)})^{p^r} + \cdots$; from which one concludes immediately that the group law of $\bar{G}$ is canonical, that $\bar{G}$ has an abelian hyperalgebra, and therefore is *abelian*, and that $\bar{X}_k^p = \bar{X}_k$ for every integer $k \geqq 0$.

As every formal Lie group over a field K can be considered as a Lie group over any extension of K, we have proved the following

THEOREM 1. *Any formal Lie group G of dimension 1 over a field K such that $X_0^p = \lambda X_0$, with $\lambda \neq 0$, is abelian.*[1] *If in addition K is algebraically closed, G is isomorphic to the multiplicative group W_1^** (with group law $(x, y) \to x + y + xy$); *moreover, there is one and only one group I_0 over K, isomorphic to W_1^*, having a canonical law and whose hyperalgebra is determined by the relations $X_h^p = X_h$ $(h = 0, 1, 2, \cdots)$.*

8. Continuing our study of one-dimensional groups, we turn now to

Case B. $X_0^p = 0$. Here, I am not able to prove that G is abelian.[1] All I can do in that direction is to prove that X_0 *commutes with every other* X_r. Indeed, suppose we have proved that X_0 commutes with $X_1, \cdots, X_{r-1}$; then X_0 commutes with the Z_α such that $\alpha < p^r$, and we can apply Lemma 1 to X_0 and X_r, obtaining

$$X_r X_0 - X_0 X_r = b X_0$$

which can also be written

$$X_r X_0 = X_0(X_r + b)$$

and from which we deduce, by induction,

$$X_r^k X_0 = X_0(X_r + b)^k$$

and in particular, for $k = p$

$$X_r^p X_0 - X_0 X_r^p = b^p X_0. \tag{30}$$

Now, one can write $X_r^p = aX_r + Y$, where Y is a linear combination of the X_α such that $\alpha < p^r$. Let σ be the isomorphism $\xi \to \xi^{p^r}$ of K onto K^{p^r}, and denote also by σ the corresponding mappings of G onto G^σ and of the hyperalgebra of G onto that of G^σ obtained by applying σ to the coefficients of the group law; it is clear that the group law of G^σ is also canonical. Now, if $\boldsymbol{p}'$ is the derived "Frobenius homomorphism [3, no. 13], apply the ring-homomorphism $\sigma^{-1} \circ \boldsymbol{p}'^r$ to the relation $X_r^p = aX_r + Y$; we obtain $X_0^p = a^{-p^r} X_0$, hence $a = 0$, and the inductive assumption shows that X_0 commutes with X_r.

Using Lemma 2, it is then possible to show that $X_1^p = cX_0$, and using Lemma 1, that $[X_1, X_2] = bX_0$; but there does not seem to be any similar argument which will prove that $b = 0$.

We will therefore *assume*, from now on, that G is abelian and has a canonical group law.[1] Suppose we have $X_0^p = X_1^p = \cdots = X_{r-1}^p = 0$; then it is clear that $Z_\alpha^p = 0$ for $\alpha < p^r$, and Lemma 2 shows that X_r^p is a *derivation*, in other words $X_r^p = bX_0$. If $b = 0$, we can go on with the induction; two cases are therefore possible:

Case B1. $X_r^p = 0$ *for every* r. These relations are obviously invariant under any isomorphism, hence we can suppose the group law of G is canonical, and then [3, formula (30)], G is the *additive group* W_1 (with group law $(x, y) \to x + y$).

Case B2. $X_0^p = X_1^p = \cdots = X_{h-1}^p = 0$, $X_h^p \neq 0$. A transformation of type $\bar{x} = \lambda x$ reduces to the case $X_h^p = X_0$. As a basis for an inductive process, suppose we have also $X_{h+1}^p = X_1, \cdots, X_{h+r-1}^p = X_{r-1}$. Apply the isomorphism $\sigma : \xi \to \xi^p$ to G. As the group law of G^σ is canonical and the constants of structure of the algebra $\mathfrak{L}_{h+r}$ are in the prime field of characteristic p, and therefore $\mathfrak{L}_{h+r}^\sigma$ is identical to $\mathfrak{L}_{h+r}$, it follows from the uniqueness theorem (see **4**), that the group laws of G and G^σ coincide modulo x^{p^r} and y^{p^r}; hence the coefficients, in the group law of G, of monomials $x^\lambda y^\mu$, where both λ and μ

are $< p^r$, belong to the prime field. Now the homomorphism $Y \to Y^p$ of the (commutative) ring $\mathfrak{s}_{h+r}$ coincides with the homomorphism $\boldsymbol{p}'^h$ on the generators X_i $(0 \leqq i \leqq h+r-1)$ of the algebra $\mathfrak{s}_{h+r}$; as the Z_α for $\alpha < p^{r+h}$ are polynomials in those X_i with coefficients in the prime field, it follows from the definition of $\boldsymbol{p}'$ and of the Z_α, that we have $Z_\alpha{}^p = 0$ if α is not a multiple of p^h, and $Z_\alpha{}^p = Z_\beta$ if $\alpha = p^h\beta$. Lemma 2 then proves that $X_{h+r}{}^p - X_r$ is a *derivation*, in other words,

$$X_{h+r}{}^p - X_r = bX_0. \tag{31}$$

We can then consider an isomorphism of type $v_1(x) = x + \lambda x^{p^r}$ on a group G_1, and we have

$$v'_1(X_k) = X_k{}^{(1)} \quad \text{for} \quad 0 \leqq k \leqq r-1$$

$$v'_1(X_r) = X_r{}^{(1)} + \lambda X_0{}^{(1)}$$

$$v'_1(X_{k+r}) = X_{k+r}{}^{(1)} + \phi_k(X_0{}^{(1)}, \cdots, X_{k-1}{}^{(1)}) + \lambda^{p^k} X_k{}^{(1)}$$

for $1 \leqq k \leqq h$, ϕ_k being a polynomial in the $X_j{}^{(1)}$. This, together with equation (31), gives $(X_{k+r}{}^{(1)})^p = X_{k+r-h}{}^{(1)}$ for $k < h$, and

$$(X_{h+r}{}^{(1)})^p - X_r{}^{(1)} = (b + \lambda - \lambda^{p^{h+1}}) X_0{}^{(1)}$$

and therefore we can choose λ such that the right-hand side vanishes. We can then, as in **7**, determine an isomorphism v_2 of G_1 onto a group $\bar{G}$ with canonical group law, such that $v'_2(X_k{}^{(1)}) = \bar{X}_k$ for $k \leqq h+r$, and in addition the isomorphism $v = v_2 v_1$ of G on $\bar{G}$ has the form $v(x) = x + \lambda x^{p^r} + \cdots$. The argument is then concluded by induction on r, as in **7**, and yields the following result:

THEOREM 2. *Let G be a one-dimensional abelian formal Lie group over an algebraically closed field K, such that $X_0{}^p = 0$. If $X_h{}^p = 0$ for every $h \geqq 0$, G is isomorphic to the additive group W_1. If on the contrary there is a smallest integer $r > 0$ such that $X_r{}^p \neq 0$, there is one and only one group I_r over K, isomorphic to G, having a canonical law, and whose hyperalgebra is determined by the relations*

$$X_k{}^p = 0 \quad \textit{for} \quad k < r, \qquad X_k{}^p = X_{k-r} \quad \textit{for} \quad k \geqq r. \tag{32}$$

9. The elliptic curves. Theorems 1 and 2 would give a complete description of all abelian Lie groups of dimension 1 over an algebraically closed field, *if we knew that for every $r > 0$ there exists a group G such that $X_k{}^p = 0$ for $k < r$ and $X_r{}^p \neq 0$.* But at present I am unable to exhibit such

groups,[1] except for the case $r=1$, $p=5$: the computations in [4] show indeed that the elliptic group $E_5(0,b)$, with $b\neq 0$, is of such a type. It seems likely that the groups I_r exist for every $r>0$ and every prime p.

It is possible to give a simple criterion for an elliptic group $E_p(a,b)$ $(p\geqq 3)$ to be isomorphic to the multiplicative group W_1^*, when K is algebraically closed. More generally, let G be a one-dimensional formal Lie group, with the group law written

$$(x,y)\to\phi(x,y)=x+v_1(x)y+v_2(x)y^2+\cdots \tag{33}$$

and

$$v_1(x)=1+a_1x+\cdots.$$

The criterion of Theorem 1 can be transformed in the following one:

PROPOSITION 4. *In order that G be isomorphic to the multiplicative group W_1^* (K being an algebraically closed field), a necessary and sufficient condition is that the coefficient of x^{p-1} in the power series $1/v_1(x)$ be different from 0.*

Indeed, we have

$$X_0=v_1D_0;$$

it follows that

$$X_0^p=((v_1D_0)^{p-1}v_1)\cdot D_0+\cdots$$

where the unwritten terms are combinations of $D_0^2, D_0^3,\cdots$; as we know that X_0^p is a derivation, these terms are in fact reduced to 0, and the constant γ such that $X_0^p=\gamma X_0$ is the constant term in the series $(v_1D_0)^{p-1}v_1$. Our assertion will then result of the following lemma:

LEMMA 3. *Let D be a derivation in a commutative algebra A of characteristic $p>0$; then, for every element z in that algebra,*

$$(zD)^{p-1}z=-zD^{p-1}(z^{p-1}). \tag{34}$$

Supposing this proved, and replacing z by v_1 and D by D_0 in (34), we see that γ is the constant term of $-D^{p-1}(v_1^{p-1})$, or equivalently, the coefficient of x^{p-1} in v_1^{p-1}; but as $v_1^p(x)=1+a_1^px^p+\cdots,\gamma$ is also the coefficient of x^{p-1} in v_1^{-1}, and this ends the proof of Prop. 4.

We are thus reduced to proving Lemma 3. I am indebted to G. Hochschild for the following proof, which is shorter and more elegant than my original one, and which I reproduce here with his kind permission.

Hochschild's proof is based on the following more general result:

LEMMA 4. *Let R be any commutative algebra over the prime field $\mathbf{F}_p$, and let δ be a derivation of R. Then, for any $r \in R$,*

$$(r\delta)^p = r^p\delta^p + (r\delta)^{p-1}(r)\delta \tag{35}$$

(here $r\delta$ stands for the derivation $x \to r\delta(x)$).

Let t and x_i $(i = 0, 1, \cdots)$ be indeterminates, and let H be the algebra of polynomials $\mathbf{F}_p[t, x_0, x_1, \cdots]$. There is a derivation τ of H such that $\tau(x_i) = x_{i+1}$, $\tau(t) = 1$. Identifying an element g of H with the multiplication $f \to gf$ by this element, we have (in the ring of endomorphisms of the vector space H)

$$\tau x_i = x_i\tau + x_{i+1}.$$

These relations show immediately that we can write

$$(x_0\tau)^p = x_0{}^p\tau^p + \sum_{i=1}^{p-1} q_i\tau^i \tag{36}$$

where the q_i are polynomials in the x_j. Applying the endomorphisms on both sides of (36) to the element t^{p-1}, we obtain (observing that $(x_0\tau)^p$ is a derivation)

$$(p-1)(x_0\tau)^p(t)t^{p-2} = \sum_{i=1}^{p-1} (p-1)\cdots(p-i)q_it^{p-1-i}.$$

This implies $q_i = 0$ for $i > 1$ and $q_1 = (x_0\tau)^p(t) = (x_0\tau)^{p-1}(x_0)$. Hence

$$(x_0\tau)^p = x_0{}^p\tau^p + (x_0\tau)^{p-1}(x_0). \tag{37}$$

Let S be the subring of the ring of endomorphisms of the vector space H, generated by τ and the multiplications by the x_i. There is a homomorphism f of S into the endomorphism ring of the vector space R, such that $f(\tau) = \delta$, $f(x_0)$ is the multiplication by r, and $f(x_i)$ the multiplication by $\delta^i(r)$ for $i \geqq 1$. Applying f to both sides of (37) yields relation (35).

Lemma 4 being proved, we now apply it to $R = \mathbf{F}_p(t, x_0, x_1, \cdots)$ (field of quotients of H), and to the derivation δ of R such that $\delta(x_i) = x_{i+1}$ and $\delta(t) = 1/x_0$. Taking the values of both sides of (35), with $r = x_0$, for the element t, gives

$$0 = x_0{}^p\delta^{p-1}(1/x_0) + (x_0\delta)^{p-1}(x_0)\cdot(1/x_0),$$

whence

$$(x_0\delta)^{p-1}(x_0) = -x_0{}^{p+1}\delta^{p-1}(1/x_0).$$

Since $\delta(x_0{}^p) = 0$, this may be written

$$(x_0\delta)^{p-1}(x_0) = -x_0\delta^{p-1}(x_0{}^{p-1}). \tag{38}$$

Now there is a homomorphism ϕ of the ring of polynomials $\boldsymbol{F}_p[x_0, x_1, \cdots]$ into the algebra A such that $\phi(x_0) = z$, $\phi(x_i) = D^i(z)$ and $\phi \circ \delta = D \circ \phi$. Applying ϕ to both sides of (38) gives (34), and this ends the proof of Lemma 3.

For the elliptic group $E_p(a, b)$ [4], we have $v_1(x) = (1 - ax^4 - bx^6)^{\frac{1}{2}}$; to say that the coefficient of x^{p-1} in $1/v_1(x)$ is $\neq 0$ means that the *Hasse invariant* [6] of the elliptic curve is $\neq 0$.[3] Hence:

COROLLARY. *Let K be an algebraically closed field of characteristic $p > 3$. In order that the elliptic group $E_p(a, b)$ be isomorphic (as a formal Lie group) to the multiplicative group W_1^*, it is necessary and sufficient that the Hasse invariant of $E_p(a, b)$ be $\neq 0$.*[4]

We add two remarks: first of all, it is clear that the isomorphisms of $E_p(a, b)$ on W_1^* will not, in general, be algebraic ones; on the other hand, the assumption that K is algebraically closed cannot be removed; we have seen for instance in [4] that if K is the prime field of characteristic 5, the group $E_5(a, b)$ cannot be isomorphic to W_1^* if $4b^4 + a^3b^2 + 2a^6 \neq 0$.

10. Cores of abelian Lie algebras. In the two following sections, we keep the assumption that K is an *algebraically closed field*. Let G be an abelian formal Lie group of dimension n, and let $\mathfrak{g}_0$ be its Lie algebra. G being abelian, the structure of $\mathfrak{g}_0$ is entirely determined by the mapping $q: X \to X^p$ of the vector space $\mathfrak{g}_0$ into itself, which is *semilinear* with respect to the automorphism $\sigma: \xi \to \xi^p$ of K. The arguments which lead to Fitting's lemma [1, p. 132] apply as well here to the mapping q: let k be the smallest integer such that $q^k(\mathfrak{g}_0) = q^{k+1}(\mathfrak{g}_0)$; then k is also the smallest integer such that $q^{-k}(0) = q^{-(k+1)}(0)$; $\mathfrak{g}_0$ is the direct sum of the two Lie algebras $\mathfrak{h} = q^k(\mathfrak{g}_0)$ and $\mathfrak{k} = q^{-k}(0)$, the restriction of q to $\mathfrak{h}$ is a *one-one and onto mapping of* $\mathfrak{h}$, and for every $X \in \mathfrak{k}$, one has $X^{p^k} = 0$, k being the smallest integer having that property. We will say that $\mathfrak{h}$ is the *core* of the Lie algebra $\mathfrak{g}_0$.

---

[3] The differential $dx/v_1(x)$ is a differential of the first kind when x is taken as an uniformizing parameter; it is known that the fact that the coefficient of x^{p-1} in this differential vanishes, is independent of the choice of the uniformizing parameter (this follows also from Prop. 4 above), and that, by using Riemann-Roch's theorem, this condition is necessary and sufficient for the existence of a function in the field having a development of the type $x^{-p} + a_0 + a_1x + \cdots$. But this last condition is equivalent to the vanishing of the Hasse invariant [6] (I am indebted to A. Weil for these precisions).

[4] If we remark that, in the clasical case, an elliptic integral defines a (local) isomorphism of the elliptic group on the *additive* group, we may consider an isomorphism of $E_p(a, b)$ on W_1^* in the present case, as an analogon to an elliptic integral.

PROPOSITION 5. *If $\mathfrak{h}\neq\{0\}$, there exists a basis $X_1,\cdots,X_m$ of the core $\mathfrak{h}$ of $\mathfrak{g}_0$ such that $X_i^p=X_i$ for $1\leqq i\leqq m$.*

We use induction on the dimension m of $\mathfrak{h}$. Let $Y\neq 0$ be an element of $\mathfrak{h}$, and let k be the smallest integer such that $Y, Y^p,\cdots,Y^{p^k}$ are linearly dependent; we have therefore

$$Y^{p^k}=\sum_{j=0}^{k-1}\lambda_j Y^{p^j} \tag{39}$$

and by definition of $\mathfrak{h}$, the λ_j cannot be all equal to 0. Let us determine an element $X_1=\sum_{j=0}^{k-1}\xi_j Y^{p^j}$ by the condition $X_1^p=X_1$; as $Y, Y^p,\cdots,Y^{p^{k-1}}$ are linearly independent, this yields the equations

$$\left\{\begin{aligned}
&\xi_0=\lambda_0\xi_{k-1}^p\\
&\xi_1=\xi_0^p+\lambda_1\xi_{k-1}^p\\
&\cdots\cdots\cdots\\
&\xi_{k-1}=\xi_{k-2}^p+\lambda_{k-1}\xi_{k-1}^p
\end{aligned}\right. \tag{40}$$

which determine completely $\xi_0,\xi_1,\cdots,\xi_{k-2}$ as functions of $t=\xi_{k-1}$, and give for t the equation

$$t=\lambda_0^{p^k}t^{p^{k+1}}+\lambda_1^{p^{k-1}}t^{p^k}+\cdots+\lambda_{k-1}t^p. \tag{41}$$

As the λ_j are not all 0, this equation has at least one root $\neq 0$ in K, which proves the existence of $X_1\neq 0$ such that $X_1^p=X_1$. Let now $Y_2,\cdots,Y_m$ constitute with X_1 a basis of $\mathfrak{h}$; we can write

$$Y_i^p=\sum_{j=2}^{m}\beta_{ij}Y_j+\gamma_i X_1 \qquad (2\leqq i\leqq m)$$

and the definition of $\mathfrak{h}$, together with the relation $X_1^p=X_1$, imply that the matrix (β_{ij}) of order $m-1$, is invertible. The inductive hypothesis proves therefore the existence of $m-1$ elements $T_2,\cdots,T_m$ which, together with X_1, constitute a basis for $\mathfrak{h}$, and are such that

$$T_i^p=T_i+\mu_i X_1 \qquad (2\leqq i\leqq m).$$

These relations can also be written

$$(T_i+\xi_i X_1)^p=(T_i+\xi_i X_1)+(\xi_i^p-\xi_i+\mu_i)X_1 \qquad (2\leqq i\leqq m).$$

It is therefore possible to choose the ξ_i $(2\leqq i\leqq m)$ in K such that the elements $X_i=T_i+\xi_i X_1$ $(2\leqq i\leqq m)$ constitute, together with X_1, a basis of $\mathfrak{h}$ satisfying the conditions of Proposition 5. The same argument may be applied to any Lie *subalgebra* of $\mathfrak{h}$; but if $Y=\sum_{i=1}^{m}\rho_i X_i$, the relation $Y^p=Y$

is equivalent to the m equations $\rho_i^p = \rho_i$, and means therefore that the coefficients ρ_i $(1 \leqq i \leqq m)$ belong to the *prime field* $\boldsymbol{F}_p$ of characteristic p. Hence:

PROPOSITION 6. *Let V be the vector space over $\boldsymbol{F}_p$ generated by $X_1, \cdots, X_m$. There is a one-to-one correspondence between the Lie subalgebras of $\mathfrak{h}$ and the subspaces of V; in particular, every subalgebra of $\mathfrak{h}$ is a direct summand.*

This shows in particular that the number of Lie subalgebras of $\mathfrak{h}$ is *finite*, and equal to the number of subspaces of V.

11. The structure of the Lie algebra $\mathfrak{k}$, supplementary to $\mathfrak{h}$ in $\mathfrak{g}_0$, is easily obtained by the Weyr-Fitting method [1]; let $s = n - m$ be the dimension of k, s_i $(1 \leqq i \leqq k)$ the dimension of $q^{i-1}(q^{-i}(0))$. The sequence $(s_i)_{1 \leqq i \leqq k}$ is decreasing, we have $s = \sum_{i=1}^{k} s_i$ and there is a basis (Y_{it}) of $\mathfrak{k}$ such that $1 \leqq i \leqq k$, $1 \leqq t \leqq s_i$ for each i, and which satisfies the following relations

$$(41) \qquad Y_{1t}^p = 0 \quad (1 \leqq t \leqq s_1), \qquad Y_{it}^p = Y_{i-1,t} \quad (2 \leqq i \leqq k, 1 \leqq t \leqq s_i).$$

We suppress the details of the proof. We will say that $\mathfrak{k}$ is the *p-radical* of the Lie algebra $\mathfrak{g}_0$.

12. Direct products. The notion of *direct product* of two formal Lie groups G_1, G_2 over K is defined in a natural way. Let n_1, n_2 be the dimensions of G_1 and G_2; it will be convenient to denote by $\alpha, \beta, \cdots$ the systems of n_1 indices, by $\lambda, \mu, \cdots$ the systems of n_2 indices, a system of $n_1 + n_2$ indices being written (α, λ); moreover, we will reserve the usual notations $x_\alpha, X_{hi}, Z_\alpha$, etc. to G_1, the corresponding notations for G_2 being $y_\lambda, Y_{hj}, T_\lambda$, etc. With these conventions, if the group laws of G_1 and G_2 are respectively

$$x_i'' = \phi_i(\boldsymbol{x}, \boldsymbol{x}') \qquad (1 \leqq i \leqq n_1)$$

$$y_j'' = \psi_j(\boldsymbol{y}, \boldsymbol{y}') \qquad (1 \leqq j \leqq n_2)$$

the group law of $G_1 \times G_2$ simply consists, by definition, in the juxtaposition of the preceding $n_1 + n_2$ formulas. It follows at once from this definition that, in the Taylor formula (2) of $G_1 \times G_2$, the operator of index α can be identified with Z_α (which means that it is the same polynomial in the X_{hi} as Z_α), the operator of index λ can be identified with T_λ; moreover, Z_α and T_λ commute, and the operator of index (α, λ) is their product $Z_\alpha T_\lambda$. We can

express these facts by saying that the hyperalgebras of G_1 and G_2 are *typical subalgebras* [3, no. 18] of the hyperalgebra of $G_1 \times G_2$, and that the latter is the *tensor product* of these two hyperalgebras. Conversely, let G be a formal Lie group of dimension $n_1 + n_2$; let us write again α for a system of $n_1 + n_2$ indices, the last n_2 of which are 0, λ for a system of $n_1 + n_2$ indices, the first n_1 of which are 0, and let us adopt conventions similar as the previous ones. Then:

PROPOSITION 7. *Suppose the operators X_α form a typical subalgebra $\mathfrak{L}$ and the operators Y_λ a typical subalgebra $\mathfrak{M}$ of the hyperalgebra $\mathfrak{G}$ of G, and that $X_\alpha Y_\lambda = Y_\lambda X_\alpha$ for every pair (α, λ). Then, if the group law of G is canonical, G is isomorphic to the direct product $G_1 \times G_2$ of two groups having respectively $\mathfrak{L}$ and $\mathfrak{M}$ as hyperalgebras.*

Indeed, we know there exist two groups G_1, G_2 having canonical group laws and whose hyperalgebras are respectively $\mathfrak{L}$ and $\mathfrak{M}$ [5, Th. 1]. If we prove that the operator of index (α, λ) in the Taylor formula (2) of G is $Z_\alpha T_\lambda$, the proposition will result from the uniqueness theorem for groups having a given hyperalgebra [5, Th. 2]. Let $U_{(\alpha,\lambda)}$ be this operator, and let us use induction on $|\alpha| + |\lambda|$. Formula (6) then gives

$$U_{(\alpha,\lambda)}(fg) = f \cdot U_{(\alpha,\lambda)} g + g \cdot U_{(\alpha,\lambda)} f + \sum (T_\mu Z_\beta f)(T_{\lambda-\mu} Z_{\alpha-\beta} g)$$

where in the summation, we let the indices range over the set $0 \leqq \beta \leqq \alpha$, $0 \leqq \mu \leqq \lambda$, with the exception of the pairs of indices $(0, 0)$ and (α, λ). On the other hand

$$T_\lambda Z_\alpha (fg) = T_\lambda \left(\sum_{0 \leqq \beta \leqq \alpha} (Z_\beta f)(Z_{\alpha-\beta} g)\right) = \sum_{\substack{0 \leqq \beta \leqq \alpha \\ 0 \leqq \mu \leqq \lambda}} (T_\mu Z_\beta f)(T_{\lambda-\mu} Z_{\alpha-\beta} g)$$

which shows that the difference $U_{(\alpha,\lambda)} - T_\lambda Z_\alpha$ is a derivation; but from the assumption that the group law is canonical, it follows that the preceding difference must be 0 if $|\alpha| + |\lambda| > 1$, and this ends our proof.

We can get rid of the assumption that the group law of G is canonical if we assume a little more about the subgroups of G:

PROPOSITION 8. *Suppose that the equations $x_i = 0$ for $i \leqq n_1$ define a subgroup G_2 of G, and that the equations $x_i = 0$ for $n_1 < i \leqq n_1 + n_2$ define another subgroup G_1 of G. Then, if $X_\alpha Y_\lambda = Y_\lambda X_\alpha$ for every pair (α, λ), G is isomorphic to the direct product $G_1 \times G_2$.*

Indeed, if we perform in the standard way the isomorphism $\boldsymbol{u}$ of G onto a group $\bar{G}$ with canonical law (no. 4), the images of G_1 and G_2 under $\boldsymbol{u}$ are defined by annihilating the coordinates of the same indices as those whose

vanishing define G_1 and G_2 respectively ([3, no. 18] and, more correctly, [5, no. 3]); moreover, the $\bar{X}_\alpha$ (resp. $\bar{Y}_\lambda$) in the hyperalgebra of $\bar{G}$ are functions of the X_β alone (resp. of the Y_μ alone), hence $\bar{G}$ satisfies all the assumptions of Proposition 7, and the conclusion follows.

The preceding definitions and results extend immediately to the product of a finite number of formal Lie groups.

13. Cores of abelian Lie groups. We can now state the following structure theorem:

THEOREM 3. *Let G be an abelian formal Lie group over an algebraically closed field, $\mathfrak{g}_0$ its Lie algebra, $\mathfrak{h}$ the core and $\mathfrak{k}$ the p-radical of $\mathfrak{g}_0$. Then, if $\mathfrak{h}$ has dimension m, G is isomorphic to the direct product of m groups isomorphic to I_0 and of a group having $\mathfrak{k}$ as its Lie algebra.*

We first observe that a linear isomorphism $\boldsymbol{u}$ of a group G on a group $\bar{G}$, with $u_i(\boldsymbol{x}) = \sum_{j=1}^{n} \alpha_{ij} x_j$, has a derived isomorphism $\boldsymbol{u}'$ such that $\boldsymbol{u}'(X_{0i}) = \sum_{j=1}^{n} \alpha_{ji} \bar{X}_{0j}$. We can therefore always suppose that the m first variables (which we shall write x_i) are such that

$$X_{0i}^{p} = X_{0i} \qquad (1 \leqq i \leqq m) \tag{42}$$

whereas the $s = n - m$ remaining variables, written y_{jt} (notations of **11**) are such that the corresponding derivations Y_{0jt} in $\mathfrak{g}_0$ satisfy

$$Y_{01t}^{p} = 0 \quad (1 \leqq t \leqq s_1), \qquad Y_{0jt}^{p} = Y_{0,j-1,t} \tag{43}$$

$$(2 \leqq j \leqq k, 1 \leqq t \leqq s_j, \sum_{j=1}^{k} s_j = s).$$

In other words, the X_{0i} constitute a basis of $\mathfrak{h}$, the Y_{0jt} a basis of $\mathfrak{k}$. We adopt moreover the conventions of **12**, writing α for a system of n indices, the last $n - m = s$ of which are 0, and λ for a system of n indices, the first m of which are 0; an arbitrary system of n indices can therefore be denoted (α, λ); the operator of index α will be written Z_α, the operator of index λ will be written T_λ, and $U_{(\alpha,\lambda)}$ will denote the operator of index (α, λ). As a basis for an inductive argument, let us suppose that G satisfies in addition the following assumptions (A_r) $(r \geqq 0)$:

a) the group law of G is canonical;

b) $X_{hi}^{p} = X_{hi}$ for $0 \leqq h \leqq r$ and $1 \leqq i \leqq m$, and for every index $\alpha = (\alpha_1, \cdots, \alpha_m, 0, \cdots, 0)$ of height $< r$, $Z_\alpha = Z_{\alpha_1} Z_{\alpha_2} \cdots Z_{\alpha_m}$, where Z_{α_i}

is the same polynomial in $X_{0i}, X_{1i}, \cdots, X_{r-1,i}$ as the operator of the same index in the Taylor formula (2) of the group I_0;

c) for $0 \leqq h \leqq r$, Y_{hjt^p} can be expressed as a polynomial in the Y_{ljt} $(l \leqq h)$ alone; and for every index λ of height $< r$, T_λ is a polynomial in the Y_{hjt} alone $(h < r)$.

We want to determine an isomorphism of G on a group which will satisfy assumptions (A_{r+1}); we proceed in several steps.

I. Let us prove first that for any index α *of height* r, Z_α is the same polynomial in the X_{hi} $(0 \leqq h \leqq r, 1 \leqq i \leqq m)$ as in the direct product of m groups identical to I_0. Using Prop. 7, we are reduced to proving that, for $p^{r-1}+1 \leqq l \leqq p^r - 1$, Z_{le_i} is equal to the polynomial $\phi_l(X_{0i}, \cdots, X_{r-1,i})$, where $\phi_l(X_0, \cdots, X_{r-1})$ is the polynomial equal to Z_l in the hyperalgebra of the group I_0. We notice that by assumption (A_r, b), $Z_{le_i} = \phi_l(X_{0i}, \cdots, X_{r-1,i})$ for $0 \leqq l \leqq p^{r-1}$; let us argue by induction on $l > p^{r-1}$. It is clear that the "Leibniz formula" (6) for $Z'_l = \phi_l(X_{0i}, \cdots, X_{r-1,i})$ can be written

$$Z'_l(fg) = f \cdot Z'_l g + g \cdot Z'_l f + \sum (V_\beta f)(W_\gamma g) \tag{44}$$

where the operators V_β and W_γ are polynomials in $X_{0i}, \cdots, X_{r-1,i}$ which depend only on the "Leibniz formulae" for the X_{hi} $(0 \leqq h \leqq r-1)$ and on the expressions of X_{hi^p} $(0 \leqq h \leqq r-1)$; as by assumption, these are the *same* as in I_0 (X_{hi} replacing X_h), the Leibniz formula (44) for Z'_l is deduced from that of Z_l (in the group I_0) by the same replacements; but then the inductive assumption shows that the difference $Z_{le_i} - Z'_l$ is a derivation, and the assumption that the group laws of G and of I_0 are canonical proves finally that $Z_{le_i} = Z'_l$.

II. We prove next that for every index λ *of height* r, T_λ is a polynomial in the Y_{hjt} alone $(h \leqq r)$. We use again the assumption that the result holds for the indices of height $< r$ (by (A_r, c)), and we use induction on the total degree $|\lambda|$. In the Leibniz formula for T_λ

$$T_\lambda(fg) = f \cdot T_\lambda g + g \cdot T_\lambda f + \textstyle\sum_{0 \leqq \mu \leqq \lambda} (T_\mu f)(T_{\lambda-\mu} g) \tag{45}$$

all the operators T_μ which intervene in the summation are polynomials in the Y_{hjt} alone. Suppose this was not true for T_λ; in the expression of T_λ there might then exist terms in the X_{hi} alone or "mixed" terms containing both the X_{hi} and Y_{hjt}. Let $T'_\lambda = \sum_\beta b_\beta X_\beta$ be the sum of the terms of the first type, $T''_\lambda = \sum_{\beta,\mu} b_{\beta\mu} X_\beta Y_\mu$ the sum of the terms of the second type, $T'''_\lambda = T_\lambda - T'_\lambda - T''_\lambda$ the sum of the terms in the Y_μ alone. Now, from

the assumption that the group law is canonical, it follows that T'_λ cannot be a derivation if the b_β are not all 0, and therefore it follows from I that $T'_\lambda(fg) - f \cdot T'_\lambda g - g \cdot T'_\lambda f$ would then be a linear combination of terms $(X_\gamma f)(X_\delta g)$ with coefficients not all 0. Similarly $T''_\lambda(fg) - f \cdot T''_\lambda g - g \cdot T''_\lambda f$ would be a linear combination of terms $(Vf)(Wg)$ where V and W are monomials such that VW contains at least one X_{hi} *and* at least one Y_{hjt}, and the coefficients of these terms would not all be 0 if the $b_{\beta\mu}$ were not all 0. Finally, it is clear that the expression $T'''_\lambda(fg) - f \cdot T'''_\lambda g - g \cdot T'''_\lambda f$ is a sum of terms of type $(Y_\mu f)(Y_\nu g)$. If we compare these results with the right hand side in (45), we see that we must have $T'_\lambda = T''_\lambda = 0$, which proves our assertion (use being made, of course, of the linear independence of the operators X_α and Y_λ).

III. From I and the study of the group I_0 made in **7**, it follows that $Z_\alpha{}^p = Z_\alpha$ for all indices α of height $\leqq r$. Lemma 2 applied to $X_{r+1,i}$ $(1 \leqq i \leqq m)$ proves therefore that the difference $X_{r+1,i}{}^p - X_{r+1,i}$ is a *derivation*; in other words, we have

$$X_{r+1,i}{}^p = X_{r+1,i} + \sum_{i'} a_{ii'} X_{0i'} + \sum_{j',t'} b_{ij't'} Y_{0j't'}. \tag{46}$$

On the other hand, II and the assumption (A_r, c) show that for all indices λ of height $\leqq r$, $T_\lambda{}^p$ is a polynomial in the Y_{hjt} $(0 \leqq h \leqq r)$ alone; from this and Lemma 2 it follows that the difference

$$Y_{r+1,j,t}{}^p(fg) - f \cdot Y_{r+1,j,t}{}^p(g) - g \cdot Y_{r+1,j,t}{}^p(f)$$

is a sum of terms of type $(Y_\mu f)(Y_\nu g)$. The same argument as in II proves then that one has

$$Y_{r+1,j,t}{}^p = Y'_{jt} + \sum_{i'} e_{jtt'} X_{0i'} \tag{47}$$

where Y'_{jt} is a polynomial in the $Y_{hj't'}$ $(h \leqq r+1)$.

We now define an isomorphism $\boldsymbol{u}$ of G on a group $\bar{G}$ such that the power series defining the inverse $\boldsymbol{u}^{-1}$ have the form

$$\begin{cases} u_i{}^{-1}(\bar{\boldsymbol{x}}) = \bar{x}_i + \sum_{i'} \xi_{ii'} \bar{x}_{i'}{}^{p^{r+1}} + \sum_{j',t'} \eta_{ij't'} \bar{y}_{j't'}{}^{p^{r+1}} \\ u_{jt}{}^{-1}(\bar{\boldsymbol{x}}) = \bar{y}_{jt} + \sum_{i'} \xi_{jtt'} \bar{x}_{i'}{}^{p^{r+1}}, \end{cases} \tag{48}$$

the coefficients having to be determined later. This gives, for the derived homomorphism $(\boldsymbol{u}^{-1})' = (\boldsymbol{u}')^{-1}$, first

$$(\boldsymbol{u}^{-1})'(\bar{X}_{hi}) = X_{hi}, \qquad (\boldsymbol{u}^{-1})'(\bar{Y}_{hjt}) = Y_{hjt}$$

for $h \leqq r$, and further

$$(49)\qquad \begin{cases} (\boldsymbol{u}^{-1})'(\bar{X}_{r+1,i}) = X_{r+1,i} + \sum_{i'} \xi_{i'i} X_{0i'} + \sum_{j',t'} \xi_{j't'i} Y_{0j't'} \\ (\boldsymbol{u}^{-1})'(\bar{Y}_{r+1,j,t}) = Y_{r+1,j,t} + \sum_{i'} \eta_{i'jt} X_{0i'}. \end{cases}$$

If we take into account formulae (43), this gives first

$$(50)\qquad \begin{aligned} (\boldsymbol{u}^{-1})'(\bar{X}_{r+1,i}{}^p - \bar{X}_{r+1,i}) &= \sum_{i'} (\xi_{i'i}{}^p - \xi_{i'i} + a_{ii'}) X_{0i'} \\ &+ \sum_{j',t'} (b_{ij't'} - \xi_{j't'i}) Y_{0j't'} + \sum_{j',t'} \xi_{j't'i}{}^p Y_{0,j'-1,t'}. \end{aligned}$$

We can therefore choose first the $\xi_{ii'}$ such that in the right hand side the coefficients of the $X_{0i'}$ are all 0. We choose next the $\xi_{j't'i}$: for $j' = k$, $1 \leqq t' \leqq s_k$ we take $\xi_{kt'i} = b_{ikt'}$, and the coefficients of the $Y_{0kt'}$ in the right hand side of (50) vanish. Suppose next the $\xi_{j't'i}$ have been determined for all values $j' > l$; then, for $1 \leqq t' \leqq s_{l+1}$, the coefficient of $Y_{0lt'}$ in (50) is $b_{ilt'} - \xi_{lt'i} + \xi_{l+1,t',i}{}^p$; for $s_{l+1} < t' \leqq s_l$, the coefficient of $Y_{0lt'}$ is simply $b_{ilt'} - \xi_{lt'i}$; in both cases, it is possible to determine $\xi_{lt'i}$ such that these coefficients vanish. Relation (50) then gives

$$(51)\qquad \bar{X}_{r+1,i}{}^p = \bar{X}_{r+1,i} \qquad (1 \leqq i \leqq m).$$

To go further, we observe that in formula (47), Y'_{jt} is the sum of a linear combination of the $Y_{r+1,j',t'}$ and of a term Y''_{jt} which is of height $\leqq r$. Moreover, if we apply to both sides of (47) the iterated Frobenius homomorphism $\boldsymbol{p}'^{r+1}$, and take into account the relations (43), we see that we have

$$Y'_{jt} = Y_{r+1,j-1,t} + Y''_{jt}$$

(where, for $j = 1$, $Y_{r+1,j-1,t}$ must be replaced by 0). We deduce from these remarks and from (49) that

$$(\boldsymbol{u}^{-1})'(\bar{Y}_{r+1,j,t}{}^p - \bar{Y}_{r+1,j-1,t}) = Y''_{jt} + \sum_{i'} (\eta_{i'jt}{}^p - \eta_{i',j-1,t} + e_{jti'}) X_{0i'}.$$

Here, we first determine the $\eta_{i'jt}$ for $j = 1$, then by induction for the successive values of $j \leqq k$, in such a way that the coefficients of the $X_{0i'}$ on the right hand side of (52) all vanish. It follows finally that we have

$$(53)\qquad \bar{Y}_{r+1,j,t}{}^p = \bar{Y}_{r+1,j-1,t} + \bar{Y}''_{jt}$$

and the group law of $\bar{G}$ satisfies assumptions (A_{r+1}) with the possible exception of (A_{r+1}, a); but the same argument as in **7** shows that this condition also can be obtained by performing a new isomorphism which will not disturb conditions b) and c).

Having achieved the passage from (A_r) to (A_{r+1}), the proof of Theorem 3 is brought to a close by the same argument as at the end of **7**; this gives an isomorphism of G onto a group whose group law is canonical and whose hyperalgebra is the tensor product of m typical subalgebras identical to the hyperalgebra of I_0, and of another typical subalgebra, whose Lie algebra is identical to $\mathfrak{k}$. The final step consists in applying Prop. 7.

14. If a group G is the direct product of a certain number of groups identical with I_0 and of a group M having a "coreless" Lie algebra, we will say that the direct product L of the groups I_0 is the *core* of G, and that M is the *p-radical* of G. These definitions are justified by the fact that L and M are *intrinsically* characterized in G, in the following sense: if $\boldsymbol{u}$ is an automorphism of G, then $\boldsymbol{u}(L) = L$ and $\boldsymbol{u}(M) = M$, or, more precisely, the $u_i(\boldsymbol{x})$ contain only the variables corresponding to L (resp. M) when the index i is the index of such a variable. This follows from the more general result:

THEOREM 4. *Let $G_1 = L_1 \times M_1$, $G_2 = L_2 \times M_2$ be two abelian Lie groups, over an algebraically closed field, such that L_1, L_2 are products of groups identical with I_0, and M_1, M_2 have coreless Lie algebras. Then, if $\boldsymbol{u}$ is a homomorphism of G_1 into G_2, $\boldsymbol{u}$ maps L_1 into L_2 and M_1 into M_2.*

If $\mathfrak{L}_1$, $\mathfrak{L}_2$, $\mathfrak{M}_1$, $\mathfrak{M}_2$ are the hyperalgebras of L_1, L_2, M_1, M_2, it will be enough (from formula (13)) to prove that $\boldsymbol{u}'(\mathfrak{L}_1) \subset \mathfrak{L}_2$ and $\boldsymbol{u}'(\mathfrak{M}_1) \subset \mathfrak{M}_2$. Let $\mathfrak{h}_1$, $\mathfrak{h}_2$ be the cores, $\mathfrak{k}_1$, $\mathfrak{k}_2$ the p-radicals of the Lie algebras of G_1 and G_2. The fact that $\boldsymbol{u}'(Z^p) = (\boldsymbol{u}'(Z))^p$ and the definition of the core and of the p-radical (**10**) show first of all that $\boldsymbol{u}'(\mathfrak{h}_1) \subset \mathfrak{h}_2$, $\boldsymbol{u}'(\mathfrak{k}_1) \subset \mathfrak{k}_2$. Let us use conventions similar to those of the preceding numbers, writing $Z_\alpha^{(1)}$, $Z_\alpha^{(2)}$, $T_\lambda^{(1)}$, $T_\lambda^{(2)}$ for operators of $\mathfrak{L}_1$, $\mathfrak{L}_2$, $\mathfrak{M}_1$, $\mathfrak{M}_2$ respectively. Suppose we have proved that $\boldsymbol{u}'(X_{hi}^{(1)})$ belongs to $\mathfrak{L}_2$ and $\boldsymbol{u}'(Y_{hjt}^{(1)})$ belongs to $\mathfrak{M}_2$ for all operators such that $h < r$; as $\boldsymbol{u}'$ is a homomorphism, it follows that $\boldsymbol{u}'(Z_\alpha^{(1)})$ belongs to $\mathfrak{L}_2$, and $\boldsymbol{u}'(T_\lambda^{(1)})$ belongs to $\mathfrak{M}_2$ for all indices α, λ of height $< r$. Now we observe that, as a consequence of formulae (53) and (43), for every element $T_\lambda^{(2)}$ of $\mathfrak{M}_2$, there is an integer e such that $(T_\lambda^{(2)})^{p^e} = 0$. On the other hand, we must have $(\boldsymbol{u}'(X_{ri}^{(1)}))^{p^e} = \boldsymbol{u}'(X_{ri}^{(1)})$ and this shows at once that $\boldsymbol{u}'(X_{ri}^{(1)})$ cannot contain terms in $T_\lambda^{(2)}$ nor "mixed" terms $Z_\alpha^{(2)} T_\lambda^{(2)}$. On the other hand, if we suppose that $\boldsymbol{u}'(Y_{rjt}^{(1)})$ is not in $\mathfrak{M}_2$, the inductive hypothesis, together with formula (14), shows, as in part II of the argument of **13**, that we would have

$$\boldsymbol{u}'(Y_{rjt}^{(1)}) = V_{jt}^{(2)} + \sum_i a_{ijt} X_{0t}^{(2)} \tag{54}$$

where $V_{jt}^{(2)}$ belongs to $\mathfrak{M}_2$. But then, raising both sides of (54) to a sufficiently high power p^e shows at once that $a_{ijt} = 0$ for all indices, and our induction may therefore proceed, which proves the theorem.

15. We will not try to study the structure of "coreless" abelian Lie groups, where a great variety of cases seem possible. For groups without radical (over an algebraically closed field), on the contrary, not only is their structure determined by Theorem 3, but it is also possible to determine completely their homomorphisms. These groups, as follows from Theorem 3, are isomorphic to direct products $(W_1^*)^n$, and we have only therefore to determine the homomorphisms of a group $(W_1^*)^m$ into a group $(W_1^*)^n$. We introduce the following convention: for any rational *p-adic integer* $\zeta = \sum_{h=0}^{\infty} \nu_h p^h$ $(0 \leqq \nu_h \leqq p-1)$ we write $(1+x)^\zeta$ for the power series

$$(1+x)^{\nu_0}(1+x^p)^{\nu_1} \cdots (1+x^{p^h})^{\nu_h} \cdots$$

which is obviously meaningful. We have then the following theorem:

THEOREM 5. *Every homomorphism* $\boldsymbol{u}$ *of a group* $(W_1^*)^m$ *into a group* $(W_1^*)^n$ *has the form*

$$1 + u_i(\boldsymbol{x}) = \prod_{j=1}^{m} (1+x_j)^{\zeta_{ij}} \qquad (1 \leqq i \leqq n) \tag{55}$$

where the ζ_{ij} *are arbitrary p-adic integers* $(1 \leqq i \leqq n, 1 \leqq j \leqq m)$.

If $\boldsymbol{u}$ is such a homomorphism, it follows from the definition of a direct product that

$$1 + u_i(\boldsymbol{x}) = \prod_{j=1}^{m} (1 + u_i(0, \cdots, 0, x_j, 0, \cdots, 0))$$

and therefore we are immediately reduced to the case $m = n = 1$ (this is merely the usual argument which determines the homomorphisms of modules which are direct sums of submodules, as "matrices" the elements of which are homomorphisms of the submodules into each other).

Let therefore u be an endomorphism of W_1^*, and suppose $u \neq 0$; let r be the smallest number h such that $u'(X_h) \neq 0$. From this definition it follows that $u'(Z_k) = 0$ for $0 < k < p^r$, and relation (14) shows therefore that $u'(X_r)$ is a *derivation,* in other words

$$u'(X_r) = \nu_r X_0, \qquad \nu_r \neq 0.$$

Raising both sides of this equation to the power p, and remembering that $X_h^p = X_h$ for every $h \geqq 0$, we see that ν_r is in the prime field $\boldsymbol{F}_p$, and therefore

can be identified with an integer such that $0 < \nu_r \leqq p-1$. If v_r is the automorphism of W_1* such that $1 + v_r(x) = (1+x)^{\nu_r}$, then it is immediate that $(v_r^{-1}u)'(X_r) = X_0$. Let us now suppose that we have $u'(X_h) = X_{h-r}$ for $r \leqq h < s$; this means that u' coincides with the iterated Frobenius homomorphism $\boldsymbol{p}'^r$ on all X_h such that $h < s$, hence if $k < p^s$, $\boldsymbol{u}'(Z_k) = 0$ if k is not a multiple of p^r, and if $k = p^r h$, $u'(Z_k) = Z_h$. This remark, together with relations (6) and (14), prove that $u'(X_s) - X_{s-r}$ is a derivation, in other words

$$u'(X_s) = X_{s-r} + \nu_s X_0.$$

Raising both sides to the power p shows that ν_s is in $\boldsymbol{F}_p$, and we identify it again with an integer such that $0 \leqq \nu_s \leqq p-1$. Then, if v_s is the automorphism of W_1* such that $1 + v_s(x) = (1+x)^{1+p^{s-r}\nu_s}$, it is immediate to see that $(v_s^{-1}u)'(X_h) = 0$ for $h < r$, $(v_s^{-1}u)'(X_h) = X_{h-r}$ for $r \leqq h < s+1$.

The proof is then concluded by the usual inductive argument and "passage to the limit": the "infinite product" $v = v_r v_{r+1} \cdots v_s \cdots$ is meaningful and has the form $1 + v(x) = (1+x)^{\zeta}$, where ζ is an invertible p-adic integer; moreover, the definition of the v_s gives $(v^{-1}u)'(X_h) = \boldsymbol{p}'^r(X_h)$ for every h; the endomorphisms $v^{-1}u$ and $\boldsymbol{p}^r$ therefore coincide, in other words $1 + u(x) = (1+x)^{p^r\zeta}$, which ends the proof.

16. Some examples. The Lie algebra of the additive Witt group W_n is easily determined by induction on n, if we observe that the mapping $\boldsymbol{u}$ such that $u_1(\boldsymbol{x}) = 0$, $u_i(\boldsymbol{x}) = x_{i-1}$ for $2 \leqq i \leqq n$, is a homomorphism of W_n into itself, the image of W_n under $\boldsymbol{u}$ being isomorphic to W_{n-1} [7]. As $\boldsymbol{u}'(X_{0i}) = X_{0,i+1}$ for $1 \leqq i \leqq n-1$, $\boldsymbol{u}'(X_{0n}) = 0$, it is easy to prove by induction that

$$X_{0i}^{p} = X_{0,i+1} \text{ for } 1 \leqq i \leqq n-1,\ X_{0n}^{p} = 0. \tag{56}$$

Indeed, relations (56) for $i > 1$ follow from the isomorphism of $\boldsymbol{u}(W_n)$ with W_{n-1}; moreover, as $\boldsymbol{u}'(X_{01}^{p} - X_{02}) = 0$, one must have $X_{01}^{p} = X_{02} + \lambda X_{0n}$, and we are reduced to showing that $\lambda = 0$. But from the definition of W_n, it follows easily that

$$X_{01} = D_{01} + w_2 D_{02} + \cdots + w_n D_{0n}$$

where the w_i have no constant term, and $w_n = x_1^{p-1}h(x_1, \cdots, x_{n-1})$, h having no constant term if $n > 2$. As $X_{0n} = D_{0n}$, the coefficient of X_{0n} in X_{01}^{p} can have no constant term if $n > 2$, hence must be 0. For $n = 2$, the relations (56) are proved by direct computation.

Relations (56) show therefore that W_n is a coreless abelian group. We

intend to return to the study of that group in another paper. With regard to the multiplicative Witt group W_n^*, we have the following result: W_n^* *is isomorphic to the direct product* $W_1^* \times W_{n-1}$. To show this, we remark that the relations $x_2 = \cdots = x_n = 0$ define in W_n^* a subgroup obviously isomorphic to W_1^*. Now, the "inverse" in the group W_1^* is given by the series $\theta(x_1) = -x_1/(1+x_1)$; it follows that the mapping $\boldsymbol{u}$ defined by $u_1(\boldsymbol{x}) = 0$, and

$$u_i(\boldsymbol{x}) = \phi_i(\theta(x_1), 0, \cdots, 0, x_1, \cdots, x_n) \qquad (2 \leqq i \leqq n)$$

(where the ϕ_i define the group law of W_n^*) is a homomorphism of W_n^* on its subgroup V_{n-1} defined by $x_1 = 0$. From this (or directly from Proposition 8) it follows that W_n^* is isomorphic to the direct product $W_1^* \times V_{n-1}$. It remains to show that V_{n-1} is isomorphic to W_{n-1}; if we remember that the group law of V_{n-1} "formalizes" the multiplication law mod. $(1+\mathfrak{p}^n)$ in the group $1+\mathfrak{p}$ of an unramified $\mathfrak{p}$-adic field [7, pp. 133-134], an explicit isomorphism of V_{n-1} on W_{n-1} will be given by the *p-adic logarithm*, where all operations in the power series are to be understood in the "vector" sense of Witt (including division by the denominators k, which are not ordinary integers, but sums—in the vector sense—of k unit vectors). We do not go into details.

Another interesting type of formal Lie groups stems from the Poincaré-E. Cartan method of defining "bilinear groups" associated with any (associative) algebra A with unit over a field K. Suppose $(a_i)_{1 \leqq i \leqq n}$ is a basis of A over K, with a_1 the unit element, and let $a_i a_j = \sum_k \gamma_{ijk} a_k$ be the multiplication table $(\gamma_{ijk} \in K)$, with $\gamma_{1jk} = \delta_{jk}$, $\gamma_{i1k} = \delta_{ik}$. If we write the multiplication formula

$$(1+z_1)a_1 + \textstyle\sum_{i>1} z_i a_i = ((1+x_1)a_1 + \sum_{i>1} x_i a_i)((1+y_1)a_1 + \sum_{i>1} y_i a_i)$$

we get a formal Lie group $G(A)$ over K:

$$(57) \qquad \begin{cases} z_1 = x_1 + y_1 + x_1 y_1 + \sum_{j>1,k>1} \gamma_{jk1} x_j y_k \\ z_i = x_i + y_i + \sum_{j>1} (x_1 y_j + y_1 x_j) + \sum_{j>1,k>1} \gamma_{jki} x_j y_k \qquad (i > 1) \end{cases}$$

If we extend the field of scalars to an overfield K', the group $G(A_{K'})$ corresponding to the extended algebra (and to the same basis (a_i)) is defined by the same formulae (57), but here isomorphisms defined by power series with coefficients in K' are of course permitted.

Let us consider only a few simple cases. Suppose first that A is a *separable* overfield of K. Then, if Ω is the algebraic closure of K, it is well known that A_Ω splits in the direct sum of n fields isomorphic with Ω, and

therefore $G(A_\Omega)$ will be isomorphic to $(W_1{}^*)^n$, from which it follows at once that the abelian group $G(A)$ has *no p-radical.* On the other hand, suppose A is an inseparable extension generated by a single element θ, satisfying the irreducible equation $\theta^{p^e} = \alpha$ over K. Then in the field Ω, we have $\alpha = \beta^{p^e}$, and therefore the algebra A_Ω has here a basis over Ω consisting of $1, a = \theta - \beta, a^2, \cdots, a^{p^e-1}$, and we have $a^{p^e} = 0$. It is immediate that the corresponding group $G(A_\Omega)$ is isomorphic to the group denoted by J in [2, no. 5], with $l = p^e$; hence $G(A)$ is here a *coreless* abelian group. These two examples justify, in some way, the term "p-radical" introduced above and the method outlined here may perhaps be of some use in the study of associative algebras over arbitrary fields.

NORTHWESTERN UNIVERSITY.

BIBLIOGRAPHY.

[1] J. Dieudonné, "Sur la réduction canonique des couples de matrices," *Bull. Soc. Math. France,* vol. 74 (1946), pp. 130-146.

[2] ———, "Sur les groupes de Lie algébriques sur un corps de caractéristique $p > 0$," *Rend. Circ. Mat. Palermo,* (2), vol. 1 (1952), pp. 380-402.

[3] ———, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$," *Comm. Math. Helv.,* vol. 28 (1954), pp. 87-118.

[4] ———, "Sur quelques groupes de Lie abéliens sur un corps de caractéristique $p > 0$," *Archiv der Math.,* vol. 5 (1954), pp. 274-281.

[5] ———, "Sur la notion de variables canoniques," *Anais Acad. Bras. de Ciencias,* (1955).

[6] H. Hasse, "Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p," *J. reine und angew. Math.,* vol. 172 (1934), pp. 77-85.

[7] E. Witt, "Zyklische Körper und Algebren der Charakteristik p vom Grad p^n," *J. reine und angew. Math.,* vol. 176 (1937), pp. 126-140.

DOUBLY STOCHASTIC MATRICES AND COMPLEX VECTOR SPACES.*

By SEYMOUR SHERMAN.

A doubly stochastic (d. s.) matrix is a matrix P such that $P_{ij} \geqq 0$, $\sum_i P_{ij} = \sum_j P_{ij} = 1$ for all i and j. A. Horn has proved

THEOREM 1. *If $y = Px$, where x, y are complex n-vectors, and P is a* d. s. *matrix, and $c_1, c_2, \cdots, c_n$ are any complex numbers, then $\sum_{i=1}^{n} c_i y_i$ lies in the convex hull of all the points $\sum_{i=1}^{n} c_i x_{\alpha i}$, $\alpha \varepsilon R^n$, where R^n is the set of all the permutations of $(1, \cdots, n)$*

and conjectured the truth of

THEOREM 2. *If x, y are complex n-vectors and $c_1, c_2, \cdots, c_n$ are any complex numbers imply that $\sum_{i=1}^{n} c_i y_i$ lies in the convex hull of the vectors $\sum_{i=1}^{n} c_i x_{\alpha i}$, $\alpha \varepsilon R^n$, then $y = Px$ where P is a* d. s. *matrix.*

In what follows Theorem 2 is established.

Let E be complex n-space. Let η represent the general complex linear functional on E ($\eta \varepsilon E^*$) and the value of η for some $x \varepsilon E$ is represented by (η, x). If we consider E as real $2n$-space, then each real linear functional ρ on E has the property that for some $\eta \varepsilon E^*$ $(\rho, x) = R(\eta, x)$, where $R(\eta, x)$ is the real part of (η, x).

LEMMA 1. *Let X be a compact convex set in E. Suppose that for each $\eta \varepsilon E^*$ $(\eta, y) \varepsilon (\eta, X) = \{(\eta, z) : z \varepsilon X\}$. Then $y \varepsilon X$.*

Proof. Since $(\eta, y) \varepsilon (\eta, X)$, it follows $R(\eta, y) \varepsilon R(\eta, X)$. But then from a standard separation theorem ([2], p. 47) it follows that $y \varepsilon X$.

If Lemma 1 is applied to the case where X is the convex hull of the vectors which are derived from x by taking all permutations of the components of x relative to a fixed complex coordinate system, then $y \varepsilon X$ for y satisfying the hypothesis of Theorem 2. Now note

* Received November 5, 1954.

LEMMA 2. *Let G be a finite collection $\{G_1, G_2, \cdots, G_n\}$ of linear transformations $E \to E$. Let $x \in E$. Denote by $K(G)$ the convex hull of G. Denote by $K(x)$ the convex hull of $Gx = \{G_1x, G_2x, \cdots, G_nx\}$. If $y \in K(x)$, then $y = Dx$ where $D \in H(G)$.*

Proof. Since $y \in K(x)$ it follows that $y = \sum_{i=1}^{n} w_i(G_ix)$, with $w_i \geqq 0$, $\sum w_i = 1$, and so $y = Dx$ with $D = \sum w_iG_i \in H(G)$. (There are extensions to the case where G is not finite but $K(x)$ is compact; since such results are not needed in the sequel they are not presented here.) The application of Lemma 2 to $y \in X$ implies that $y = Dx$ with x, y elements of the complex vector space E and D an n by n d. s. matrix (since D is a convex combination of permutation matrices). This establishes Theorem 2.

UNIVERSITY OF PENNSYLVANIA.

REFERENCES.

[1] A. Horn, "Doubly stochastic matrices and the diagonal of a rotation matrix," *American Journal of Mathematics*, vol. 76 (1954), pp. 620-630.

[2] W. Fenchel, "Convex cones, sets and functions," Princeton University Logistics Research Project, September, 1953.

ON COVARIANT FIBERINGS OF KLEIN SPACES.*[1]

By G. D. Mostow.

---

1. Introduction. By a Klein space we mean a space on which a Lie group of transformations operates transitively; or what is equivalent, the factor space G/S of a Lie group G by a closed subgroup S. If the group G is compact then, of course, G/S is compact, but not conversely. In case G is compact, we call the Klein space G/S compact-by-heredity or "h-compact." This paper is devoted to investigating the relation between general Klein spaces and h-compact spaces.

In the special case that the isotropy group (i. e., the set of transformations keeping a point fixed) consists of the identity alone, the Klein space is a group manifold and it is known that a connected Lie group is topologically a direct product of a compact subgroup and a Euclidean space. This fact raises the question: to what extent does a similar theorem hold for general Klein spaces? Examples show readily that such a result does not hold for Klein spaces when the isotropy subgroup is not connected. When, however, the isotopy subgroup is connected, there is a similar relation. For we can prove (cf. Theorem 3.1) the theorem that a Klein space H with connected isotropy group can be retracted by a strong deformation retraction to a subspace that is homeomorphic to an h-compact Klein space. Nevertheless, it is false that a general Klein space with connected isotropy group is a direct product of a compact subspace and a Euclidean space. This is shown by an example due to Samelson (cf. Section 5).

Instead, the kind of decomposition that seems to occur is that of *covariant fibering*. If H is a Klein space with associated group G, we mean by a G-covariant fibering a decomposition of the differentiable manifold H into Euclidean fibers such that 1) the fibers are permuted transitively by some maximal compact subgroup M of G and 2) the subgroup of M which keeps some fiber F invariant is equivalent to a linear group on F. Under these circumstances, some orbit of M is a cross-section set to the fibering

---

* Received February 19, 1954; revised October 18, 1954.

[1] Research performed in part under contract DA-36-034-ORD-1274 with Office of Ordnance Research, U. S. Army.

and it is of course an h-compact subspace to which H can be retracted via a strong deformation retraction along the fibers.

We devote this paper to the existence and uniqueness of covariant fiberings of Klein spaces. Our main results are:

THEOREM. *Any two G-covariant fiberings of a Klein space are equivalent, in the sense that there exists a one-to-one bundle map of one onto the other* (Section 7).

THEOREM 4.1. *A Klein space with associated group G whose isotropy subgroup is connected and self-adjoint modulo the radical of G admits a covariant fibering.*

Theorem 4.1 applies when the connected isotropy subgroup is either semi-simple, or compact, or in the radical. In particular, the theorem holds for solvmanifolds.

Theorem 4.1 depends on a new decomposition theorem for matrices that was derived by the author in [10]. In all probability the self-adjoint hypothesis can be dropped. This would entail proving a generalization of the cited decomposition theorem for matrices.

Our method for proving the existence of covariant fiberings consists in deriving decompositions for Lie groups, some of which have independent interest. For example:

THEOREM 2.2. *Let G be a connected Lie group. Then it contains a maximal compact subgroup M and a Euclidean subspace U such that $G = M \cdot U$ topologically, and $mUm^{-1} \subset U$ for all m in M.*

As a result of this theorem, we obtain the following sharpened form of the theorem on conjugacy of compact subgroups.

THEOREM 2.3. *Let M_1 and N_1 be compact subgroups of a connected Lie group G and let θ_1 be an inner automorphism of G which sends M_1 onto N_1. Let M and N be arbitrary maximal compact subgroups of G which include M_1 and N_1 respectively. Then there is an inner automorphism θ sending M onto N and coinciding with θ_1 on M_1.*

As an application of our results on covariant fiberings we prove the

THEOREM. *An aspherical Klein space is homeomorphic to Euclidean space.*

This result can be generalized to obtain a characterization of Euclidean space as an aspherical space whose group of auto-homeomorphisms contains a locally compact C_σ transitive subgroup (to appear).

2. Some decompositions for Lie groups.

Notation. Lie groups and their Lie algebras are denoted by corresponding Roman and German letters. $\mathfrak{G}$, the Lie algebra of G, is identified with the tangent space to G at the identity.

Let $\mathfrak{L}$ be a real semi-simple Lie algebra, i.e., one on which the Killing form $\operatorname{Tr} \operatorname{ad} X \operatorname{ad} Y$ is non-degenerate; or equivalently, one having no abelian ideals. By the adjoint group of $\mathfrak{L}$ we mean the connected Lie group of automorphisms of $\mathfrak{L}$ whose Lie algebra is $\operatorname{ad} \mathfrak{L}$. A subalgebra $\mathfrak{K}$ is called a compact subalgebra of $\mathfrak{L}$ if the analytic subgroup of the adjoint group with Lie algebra $\operatorname{ad} \mathfrak{K}$ is compact. It is known that if $\mathfrak{K}$ is a maximal compact subalgebra of $\mathfrak{L}$, then it has a unique orthogonal complement $\mathfrak{E}$ with respect to the Killing form (cf. [9]); moreover, if ρ is any representation of $\mathfrak{L}$ by linear transformations of a real linear space V, there is a base for V with respect to which $\rho(\mathfrak{K})$ and $\rho(\mathfrak{E})$ consist of skew-symmetric and symmetric matrices respectively (cf. [10]). To each maximal compact subalgebra $\mathfrak{K}$ there corresponds a unique automorphism $\theta_{\mathfrak{K}}$ of order two such that $\theta_{\mathfrak{K}}(X) = X$ or $-X$ according as X is in $\mathfrak{K}$ or $\mathfrak{E}$. We call $\theta_{\mathfrak{K}}$ the "$\mathfrak{K}$-star" automorphism of $\mathfrak{L}$.

Definition. A subalgebra of a real semi-simple algebra $\mathfrak{L}$ is called *self-adjoint in* $\mathfrak{L}$ if it is invariant under some star automorphism of $\mathfrak{L}$.

To say that the subalgebra $\mathfrak{C}$ is invariant under the $\mathfrak{K}$-star automorphism of $\mathfrak{L}$ is equivalent to $\mathfrak{C} = \mathfrak{C} \cap \mathfrak{K} + \mathfrak{C} \cap \mathfrak{E}$ where $\mathfrak{E}$ is the orthogonal complement of $\mathfrak{K}$. The author has proved in [10] that a semi-simple subalgebra of a semi-simple $\mathfrak{L}$ is self-adjoint in $\mathfrak{L}$.

Let L be a connected semi-simple group, C an analytic subgroup. We say that C is self-adjoint in L if the Lie subalgebra $\mathfrak{C}$ is self-adjoint in $\mathfrak{L}$. If G is a connected Lie group, C is an analytic subgroup, and R is the radical of G, we say that C is *self-adjoint modulo the radical* if CR/R is self-adjoint in the semi-simple group G/R.

It is convenient to know that a star automorphism of the Lie algebra of a semi-simple analytic group can be extended to an automorphism of the group. For let D be the center of the simply connected group L^* with semi-simple Lie algebra $\mathfrak{L}$, and let $\mathfrak{K} + \mathfrak{E}$ be a Cartan decomposition of $\mathfrak{L}$. Then D is contained in the analytic subgroup determined by K (cf. [9]). Now L^* being simply connected, the $\mathfrak{K}$-star automorphism of $\mathfrak{L}$ extends to an automorphism θ of L^*, and by the foregoing θ keeps the points of D fixed.

Hence θ induces an automorphism of any analytic group L locally isomorphic with L^*—we call it the K-star homomorphism of L, where K is the analytic subgroup of L determined by $\mathfrak{K}$.

It is clear that C is self-adjoint in L if and only if it is invariant under some star automorphism of the group L.

LEMMA 2.1. *Let $\mathfrak{C}$ be a self-adjoint subalgebra of the semi-simple Lie algebra $\mathfrak{L}$ and let $\mathfrak{R}$ be the radical of $\mathfrak{C}$. Let θ be a star-automorphism of $\mathfrak{L}$ which keeps $\mathfrak{C}$ invariant and let θ' denote the induced automorphism of $\mathfrak{C}/R$. Then θ' is a star-automorphism of $\mathfrak{C}/R$.*

Proof. Let θ be the $\mathfrak{K}$-star automorphism. Then $\mathfrak{L} = \mathfrak{K} + \mathfrak{E}$ and furthermore, coordinates may be selected in $\mathfrak{L}$ so that the matrix of $\operatorname{ad} X$ is skew-symmetric if $X \in \mathfrak{K}$, symmetric if $X \in \mathfrak{E}$ (cf. [9] or [10]). Now $\theta(\mathfrak{C}) = \mathfrak{C}$ implies $\mathfrak{C} = \mathfrak{C} \cap \mathfrak{K} + \mathfrak{C} \cap \mathfrak{E}$ and hence $\operatorname{ad} \mathfrak{C}$ (considered as a subset of $\operatorname{ad} \mathfrak{L}$) is represented by a self-adjoint family of matrices. As a result $\operatorname{ad} \mathfrak{C}$ is a completely reducible family. Operating with $\operatorname{ad} \mathfrak{C}$ on the radical $\mathfrak{R}$, we find that $\mathfrak{R}$ is a direct sum of $\mathfrak{C}$-ideals and is thus abelian. Operating with $\operatorname{ad} \mathfrak{C}$ on $\mathfrak{C}$, we find that $\mathfrak{R}$ admits a complementary ideal and thus $\mathfrak{R}$ is central in $\mathfrak{C}$. It follows at once that $\mathfrak{C} = [\mathfrak{C}, \mathfrak{C}] + \mathfrak{R}$ (direct), and $[\mathfrak{C}, \mathfrak{C}]$ may be identified with the semi-simple quotient $\mathfrak{C}/\mathfrak{R}$. Let us denote $[\mathfrak{C}, \mathfrak{C}]$ by $\mathfrak{M}$. $\mathfrak{M}$ is invariant under θ and the automorphism θ' can obviously be identified with the restriction of θ to $\mathfrak{M}$. Now $\mathfrak{M} = \mathfrak{M} \cap \mathfrak{K} + \mathfrak{M} \cap \mathfrak{E}$ and $\theta'(X)$ is X if $X \in \mathfrak{M} \cap \mathfrak{K}$ and $-X$ if $X \in \mathfrak{M} \cap \mathfrak{E}$. Furthermore, $\mathfrak{M} \cap \mathfrak{K} + \mathfrak{M} \cap \mathfrak{E}$ is a Cartan decomposition of $\mathfrak{M}$ (cf. [10]). Consequently θ' is a star automorphism.

Let Γ be a group of automorphisms of a Lie group G and let S be a subset of G. Let $d\Gamma$ denote the set of differentials at the identity of the transformations of Γ, that is, the automorphisms of $\mathfrak{G}$ induced by Γ.

Definition. S is a Γ-*invariant exp-set* if there exist linearly independent subspaces $\mathfrak{S}_1, \cdots, \mathfrak{S}_n$ of $\mathfrak{G}$ which are invariant under $d\Gamma$ such that the mapping $s_1 + s_2 + \cdots + s_n \to \exp s_1 \cdot \exp s_2, \cdots, s_n$ is a homeomorphism of $\mathfrak{S}_1 + \cdots + \mathfrak{S}_n$ onto S (s_i in S_i). Γ is called completely reducible if $d\Gamma$ is a completely reducible (linear) group.

It should be noticed that a Γ-invariant exp-set S is invariant under Γ and homeomorphic to Euclidean space; also that the operation of Γ on S is equivalent to the operation of $d\Gamma$ on a linear subspace of $\mathfrak{G}$. These facts result from the well-known identity $T(\exp X) = \exp dT(X)$, for X in $\mathfrak{G}$. These facts result from the well-known identity $T(\exp X) = \exp dT(X)$, for

X in $\mathfrak{G}$ and any automorphism T, where dT denotes the differential of T at the identity.

If M is a subgroup of a Lie group G and Γ_M denotes the set of inner automorphisms of G by elements of M, we shall mean by an *M-invariant exp-set* a Γ_M-invariant exp-set.

LEMMA 2.2. *Let G be a connected Lie group containing no non-trivial central toroidal subgroup. Let $\mathfrak{N}$ be the maximum nilpotent ideal of the radical $\mathfrak{R}$. Then N is a closed simply connected subgroup of G.*

Proof. It is clear that the radical R is a closed subgroup of G. Inasmuch as N is the connected component of the identity in the set of all elements x of R such that $\mathrm{Ad}\,x$ has only 1 as eigenvalue ($\mathrm{Ad}\,x$ being the differential at the identity I of the inner automorphism $g \to xgx^{-1}$), it is clear that N is closed. For any non-zero X in $\mathfrak{N}$, $\exp X \neq I$. Otherwise $\mathrm{ad}\,X$ which is nilpotent on G and satisfies $\exp X = \mathrm{Ad}\exp X = 1$ must be equal to $\log \exp \mathrm{ad}\,X = \log 1 = 0$; that is, X is central in G and the one parameter subgroup $\{\exp tX \mid 0 \leqq t \leqq 1\}$ is a compact toroid, contrary to our assumption.

Now let N denote the simply connected covering space of N, let D be the kernel of the natural map of N onto N, and let us identify the Lie algebra of N with N. Since any element of a nilpotent group lies on a one-parameter subgroup (this is well-known, cf. [7] or [11]) for any x in D, there is an X in N such that $\exp X = x$ is in D. Since $\exp X = I$ in N, we conclude $X = 0$, $x = I$, $D = (I)$, and N is simply connected.

Definition. Let G be a topological group and let $A_1, \cdots, A_n$ be subspaces. We say that $G = A_1 \cdot A_2 \cdots A_n$ topologically if the mapping $\theta: (a_1, \cdots, a_n) \to a_1 a_2 \cdots a_n$ of $A_1 \times \cdots \times A_n$ into G is a homeomorphism onto, each A_i being given its relative topology with respect to G.

PROPOSITION 2.1. *Let G be an analytic group with non-trivial radical R and let C be a closed analytic subgroup. Assume that for every non-trivial abelian normal analytic subgroup V the topological closure of CV is G. Then there is a normal abelian analytic subgroup W such that $G = CW$.*

Proof. For typopgraphical convenience, we denote the topological closure of a set S by $\mathfrak{Cl}\,S$.

We let G^* denote the simply connected covering group of G, f the covering homomorphism and D^* the kernel of f. For any analytic subgroup S of G we denote by S^* the connected component of the identity of $f^{-1}(S)$ and vice versa, and we denote the Lie subalgebra of both by $\mathfrak{S}$. We denote

by $[S, S]$ the commutator subgroup of S, it being the analytic subgroup with Lie algebra $[\mathfrak{S}, \mathfrak{S}]$.

From the hypotheses of the proposition it follows directly that for any non-trivial normal analytic abelian subgroup V (such a V exists since G is not semi-simple), $G = \mathfrak{Gl}\, D^*C^*V^*$. Since

$$[\mathfrak{Gl}\, D^*C^*V^*, \mathfrak{Gl}\, D^*C^*V^*] \subset \mathfrak{Gl}\, [D^*C^*V^*, D^*C^*V^*] \subset \mathfrak{Gl}\, [C^*V^*, C^*V^*],$$

we conclude that $[G^*, G^*] \subset \mathfrak{Gl}\, [C^*V^*, C^*V^*]$.

Now C^*V^* is a normal analytic subgroup of G^* since its Lie algebra is clearly invariant under $\mathrm{Ad}\, G^*$ and hence an ideal; hence $[C^*V, C^*V^*]$ is a normal analytic subgroup of the simply connected Lie group G^*. Hence $[C^*V^*, C^*V^*]$ is closed (cf. Pontriagin, *Topological Groups*, p. 279). Thus $[G^*, G^*] \subset [C^*V^*, C^*V^*]$ (cf. [7]). It follows now from the fact that a semi-simple Lie algera is its own commutator subalgebra that $G^*/R^* = [G^*, G^*]R^*/R^* \subset C^*R^*/R^*$. Hence $G^* = C^*R^*$. Letting S^* denote the radical of C^* and $L^* \cdot S^*$ a Levi decomposition of C^*, we conclude that $G^* = L^* \cdot R^*$ is a Levi decomposition of G^*. Inasmuch as G^* is simply connected and admits as a covering group a semi-direct product of L^* and R^*, we conclude that $G^* = L^* \cdot R^*$ (semi-direct) and in particular $L^* \cdot R^*$ is a direct product fibering of G^*.

We now set $D_L{}^* = D^*R^* \cap L^*$, $D_R{}^* = D^*L^* \cap R^*$. Since $x \to xR^* \cap L^*$ is a homomorphism of G^* onto L^*, $D_L{}^*$ is central in L^*; since $d \to dL^* \cap R^*$ is a homomorphism of D^* into R^*, $D_R{}^*$ is an abelian subgroup of R^*. Furthermore, from the well-known fact that D^* is a finitely generated group, it follows that $D_R{}^*$ is finitely generated though it is, of course, not necessarily closed. Let $\rho(x)$ denote the restriction to the Lie algebra of R^* of $\mathrm{Ad}\, x$ for x in G^*. Then $\rho(L^*)$ is a semi-simple Lie group of matrices and it is known (cf. Mostow, *Annals of Mathematics*, vol. 52 (1950), p. 615) that its center is finite. Now for any r in $D_R{}^*$, there is an l in $D_L{}^*$ such that $lv \in D^*$, and an n such that $\rho(l^n) = I$, the identity. Since $lrl^{-1} = l^{-1}(lr) = r$, l and r commute. Consequently, $\rho(r^n) = \rho(l^n)\rho(r^n) = \rho(l^nr^n) = \rho((lr)^n) = I$ and r^n is central in R. Since $D_R{}^*$ is finitely generated, it contains a subgroup $D_R{}'$ of finite index which is central in R. In particular, $\mathfrak{Gl}\, D_R{}'M$ and $\mathfrak{Gl}\, D_RM$ have the same connected component of the identity for any analytic subgroup M of R^*.

Now we have for any normal analytic abelian subgroup V (which is of necessity in the radical R),

$$G^* = \mathfrak{Gl}\, D^*C^*V^* = \mathfrak{Gl}\, L^* \cdot D_R{}^*S^*V^* = L^* \cdot \mathfrak{Gl}\, D_R{}^*S^*V^*,$$

since $L^* \cdot R^*$ is a direct product fibering. Hence $R^* = \mathfrak{Cl}\, D_R^* S^* V^*$ and R^* being connected, $R^* = \mathfrak{Cl}\, D_R' S^* V^*$.

Case 1. The center Z^* of R^* is not discrete.

Here Z^* contains a non-trivial abelian normal subgroup of G^* and hence $R^* = \mathfrak{Cl}\, D_R' S^* Z^* = \mathfrak{Cl}\, S^* Z^*$. Hence S^* is normal in R^* and being invariant under conjugations by elements of L^*, we conclude that S^* is normal in G^*. If $S^* =$ (identity), then $R^* = Z^*$, R is an abelian normal analytic subgroup and $G = CR$. If S^* is not trivial, it contains a characteristic abelian normal non-trivial subgroup V^*, namely, the last non-trivial subgroup in the sequence of successive commutator subgroups. Then $V = f(V^*)$ is normal in G and $G = \mathfrak{Cl}\, CV = \mathfrak{Cl}\, C = C$. Thus, the proposition is true in Case 1 ($W = R$ or $W =$ (identity)).

Case 2. The center of R^* is discrete.

Here $\mathfrak{R}$, the Lie algebra of R^*, has zero as center and hence it is not nilpotent. We denote by $\mathfrak{R}^2$ the derived algebra $[\mathfrak{R}, \mathfrak{R}]$ and recursively set $\mathfrak{R}^n = [\mathfrak{R}^{(n-1)}, \mathfrak{R}]$ and $\mathfrak{R}^\infty = \bigcap_n \mathfrak{R}^n$. $\mathfrak{R}^\infty = \mathfrak{R}^N$ for some N, and $\mathfrak{R}$ being non-nilpotent, $\mathfrak{R}^\infty \neq 0$. We denote by $\mathfrak{R}^{(n)}$ the ideal $[\mathfrak{R}^{(n-1)}, \mathfrak{R}^{(n-1)}]$ where $\mathfrak{R}^{(2)} = \mathfrak{R}^2$.

Case 2a. $[\mathfrak{R}, \mathfrak{R}]$ is not abelian.

Here $\mathfrak{R}^{(3)}$ is a non-zero characteristic ideal of $\mathfrak{G}$, the Lie algebra of G. Hence it contains a non-zero abelian ideal $\mathfrak{V}$ of G, whose corresponding subgroup in G^* we denote by V^*. From $R^* = \mathfrak{Cl}\, D_R' S^* V^*$ we infer

$$[R^*, R^*] = \mathfrak{Cl}\, [S^* V^*, S^* V^*] = [S^* V^*, S^* V^*],$$

the last assertion following since a normal analytic subgroup of a simple connected group is closed. Letting S denote the Lie algebra of S^*, we get

$$[\mathfrak{R}, \mathfrak{R}] = [\mathfrak{S}, \mathfrak{S}] + [\mathfrak{S}, \mathfrak{V}] = [\mathfrak{S}, \mathfrak{S}] + [\mathfrak{R}, \mathfrak{R}]^2. \tag{A}$$

Now it is a well-known consequence of Lie's theorem on solvable Lie algebras that $[\mathfrak{R}, \mathfrak{R}]$ is a nilpotent Lie algebra. From equation (A) it follows readily that the subalgebra $[\mathfrak{S}, \mathfrak{S}]$ must coincide with the nilpotent $[\mathfrak{R}, \mathfrak{R}]$. Hence $[\mathfrak{R}, \mathfrak{R}] \subset \mathfrak{S}$, and C contains a non-trivial abelian normal analytic subgroup of G, namely, the smallest non-trivial $[R, R]^{(n)}$. Hence $G = \mathfrak{Cl}\, CV = \mathfrak{Cl}\, C = C$, and the proposition holds in Case 2a.

Case 2b. $[\mathfrak{R}, \mathfrak{R}]$ is abelian.

Let $\mathfrak{C}$ denote the Lie subalgebra of C^*. Since $R^* = \mathfrak{Cl}\, D_R' S^* [R^*, R^*]$,

$S^* \cap [R^*, R^*]$ is clearly a normal subgroup of R^*. Thus $\mathfrak{S} \cap [\mathfrak{R}, \mathfrak{R}] = \mathfrak{C} \cap [\mathfrak{R}, \mathfrak{R}]$ is an abelian ideal of $\mathfrak{G}$ in this case. Moreover, this ideal can be assumed to be zero, for otherwise our proposition would follow trivially.

Thus we suppose without loss of generality that $\mathfrak{S} \cap [\mathfrak{R}, \mathfrak{R}] = (0)$. Here $\mathfrak{S}$ is abelian. Furthermore, S^* clearly contains a regular element of R^* and thus $\mathfrak{S}$ contains a regular element X of $\mathfrak{R}$ (cf. [11]). Let $\mathfrak{A}$ be the subset of $\mathfrak{R}$ which is annihilated by some power of $\operatorname{ad} X$. As is well-known, $\mathfrak{A}$ is a Cartan subalgebra of $\mathfrak{G}$, and as such, is its own normalizer. It is proved in [11] that $\mathfrak{G} = \mathfrak{A} + \mathfrak{R}^\infty$ with $\mathfrak{A} \cap \mathfrak{R}^\infty \subset [\mathfrak{R}^\infty, \mathfrak{R}^\infty]$. Hence we have here $\mathfrak{G} = \mathfrak{A} + \mathfrak{R}^\infty$ (semi-direct) with $\mathfrak{A} \supset \mathfrak{S}$.

Let A^* be the subgroup of G^* which corresponds to $\mathfrak{A}$. Then clearly A^* is the connected component of the identity of its normalizer $N(A^*)$. We assert now that A^* coincides with $N(A^*)$. To prove this we need only show that $N(A^*) \cap R^{*\infty}$ is connected, since $R^* = A^* \cdot R^{*\infty}$. Now let x be in $N(A^*) \cap R^{*\infty}$, and let X be an element of the Lie subalgebra R such that $\exp X = x$. Denoting by $\alpha(x)$ the restriction to $\mathfrak{R}$ of $\operatorname{ad} X$, we have that $\alpha(X)$ is nilpotent and $\exp \alpha(X)$ keeps $\mathfrak{A}$ invariant. Hence $\alpha(X) = \log \exp \alpha(X)$ keeps A invariant and thus $\alpha(\exp tX) = \exp t\alpha(X)$ keeps $\mathfrak{A}$ invariant for every t and $N(A^*)$ contains a connected subgroup through x. From this it follows that $N(A^*) \cap R^*$ is connected as well as discrete, and is thus {identity}. It follows that $N(A^*) = A^*$.

Knowing this, we assert that $D_R{}^* \subset A^*$. For from the definition of $\mathfrak{A}$, it is seen to be the centralizer of $\mathfrak{C} \cap \mathfrak{R}$ in $\mathfrak{R}$ and it is hence invariant under $\operatorname{Ad} L^*$. Hence $\operatorname{Ad} D_R{}^*(\mathfrak{A})$ $\operatorname{Ad} D^* \cdot \operatorname{Ad} D_L(\mathfrak{A}) \subset \mathfrak{A}$ and thus $D_R{}^* \subset N(A^*) = A^*$.

Inasmuch as $G^* = L^* \cdot A^* \cdot R^{*\infty}$ topologically and $D^* \subset D_L{}^* D_R{}^* \subset L^* A^*$, we conclude that $G = (LA) \cdot R^\infty$ (semi-direct), where $L = f(L^*)$ and $A = f(A^*)$, $C \subset L \cdot A$ and, in addition, R^∞ is an abelian simply connected normal analytic subgroup that is non-trivial. Hence by hypotheses, $G = \mathfrak{L} CR^\infty$. But the foregoing topological fibering of G yields $\mathfrak{L} CR^\infty = (\mathfrak{L} C) \cdot R^\infty = C \cdot R^\infty$. Hence $G = CR^\infty$, and Proposition 2.1 holds with $W = R^\infty$. Proof of Proposition 2.1 is now complete.

Note. The subgroup W of Proposition 2.1 can be taken to be non-trivial. For if W were trivial, we would have $G = C$. Since G has a non-trivial radical R, it contains a non-trivial normal abelian analytic subgroup W', namely, the last non-trivial subgroup in the sequence of successive commutator subgroups of R. Replacing W by W', our assertion follows.

THEOREM 2.1. *Let G be a connected Lie group, and C a closed connected subgroup which is self-adjoint in G modulo the radical. Let M_C be a*

maximal compact subgroup of C and let M be a maximal compact subgroup of G which includes M_C. There exist M_C-invariant exp-sets F and E such that $C = M_C \cdot E$ and $G = M \cdot F \cdot E$ topologically.

Proof is by induction on the dimension of G. We consider three cases, the third one being the case of trivial radical.

Case 1. G contains a non-trivial central toroid subgroup T.

By the induction hypothesis $G^* = G/T = M^* \cdot F^* \cdot E^*$ topologically where F^* and E^* are M_C^* $(= M_C T/T)$-invariant exp-sets, $C^* = CT/T = M_C^* \cdot E^*$, and $M^* = MT/T$. We know that F^* arises out of independent M_C^*-invariant linear subspaces $\mathfrak{F}_1^*, \cdots, \mathfrak{F}_p^*$ and that E^* arises similarly out of $E_1^*, \cdots, E_q^*$. Let ϕ denote the homeomorphism of G onto G^*, and let $\mathfrak{F}_i = d\phi^{-1}(\mathfrak{F}_i^*)$, $\mathfrak{E}_j = d\phi^{-1}(\mathfrak{E}_j^*)$ for each i, j. Clearly, each $\mathfrak{F}_i$, $\mathfrak{E}_j$, is invariant under the compact linear group $\operatorname{Ad} M_C$. Let $\mathfrak{F}_i$ be an $\operatorname{Ad} M_C$ invariant complement to $\mathfrak{T}$ in $\mathfrak{F}_i$, and let $\mathfrak{E}_j$ be an $\operatorname{Ad} M_C$ invariant complement to $\mathfrak{T}$ in $\mathfrak{E}_j$ which is also included in $\mathfrak{C} \cap \mathfrak{E}_j$ for each i and j. That $\mathfrak{E}_j$ can be so chosen follows from the fact that $\mathfrak{C} \cap \mathfrak{E}_j$ is $\operatorname{Ad} M_C$ invariant and spans $\mathfrak{E}_j$ together with $\mathfrak{T}$. Clearly $d\phi$ is bi-unique on each $\mathfrak{F}_i^*$ and $\mathfrak{E}_j^*$. Set $F = \exp \mathfrak{F}_1 \cdot \cdots \exp \mathfrak{F}_p$ and $E = \exp \mathfrak{E}_1 \cdot \cdots \exp \mathfrak{E}_q$. From $G^* = (MFE)^* = \phi(MFE)$, we deduce $G = MFET = MTFE = MFE$. To prove that $G = M \cdot F \cdot E$ topologically, we must prove that the mapping $\theta: (m, f, e) \to mfe$ of $M \times F \times E$ onto G is a homeomorphism.

θ is one-to-one. For knowing that $G^* = M^* \cdot F^* \cdot E^*$ topologically, it is sufficient to prove that ϕ is bi-unique on F and E.

Knowing that $F^* = \exp \mathfrak{F}_1^* \cdot \cdots \exp \mathfrak{F}_p^*$ topologically, it is sufficient in order to prove that ϕ is bi-unique on each $\exp \mathfrak{F}_i$.

Suppose therefore that $f_i = \exp X_i$ $(i = 1, 2)$ with X_i in $\mathfrak{F}_h$ and $\phi(f_1) = \phi(f_2)$. Then $\exp d\phi(X_1) = \phi(\exp X_1) = \phi(\exp X_2) = \exp d\phi(X_2)$ where $d\phi$ is the differential of ϕ at the identity. Since $d\phi$ is one-to-one on $\mathfrak{F}_h$ by choice of $\mathfrak{F}_h$, and exp is one-to-one on $d\phi(\mathfrak{F}_h) = \mathfrak{F}_h^*$, we conclude $X_1 = X_2$ and $f_1 = f_2$. Similarly ϕ is bi-unique on E.

It follows as point out above that the mapping θ is one-to-one. That θ is open as well as continuous follows from the invariance of domain theorem for Euclidean space applied to the locally Euclidean space $M \times F \times E$ whose dimension is the same as the dimension of G. Thus θ is a homeomorphism and $G = M \cdot F \cdot E$ topologically. Since $\phi(C) \subset M^* \cdot E^*$ and $T \subset M$, we have $C \subset ME$ and hence $C = (C \cap M) \cdot E$ topologically. Since $C \cap M = M_C$, we have $C = M_C \cdot E$ topologically.

Case 2. G has no non-trivial central toroidal subgroup but has a non-trivial radical.

Case 2a. There exists a non-trivial abelian analytic normal V with CV closed.

Let R denote the radica of G and let N denote the analytic subgroup corresponding to the maximum nilpotent ideal of R. By Lemma 2.2, N is a closed simply connected subgroup of G. V is included in N. Since N is simply connected, the analytic subgroup V is simply connected (cf. [4]) and therefore V is a non-trivial vector group. We now apply the induction hypothesis to $G^* = G/V = M^* \cdot F^* \cdot E^*$ where F^* and E^* are $M_C{}^*$-invariant exp-sets, and $C^* = CV/V = M_C{}^* \cdot E^*$ topologically, M_C being $M \cap C$, and M^* denoting MV/V.

Let ϕ denote the homomorphism of G onto G^*. Clearly $\phi(M_C) \subset M_C{}^*$. Following the procedure used in Case 1 we can define M_C-invariant exp-sets F' and E' which map bi-uniquely onto F^* and E^*. Let $\mathfrak{V}_1$ denote an $\mathrm{Ad}\, M_C$-invariant subspace of the abelian Lie algebra $\mathfrak{V}$ which is a complement to $\mathfrak{C} \cap \mathfrak{V}$ in $\mathfrak{V}$, and let V_1 denote the corresponding vector subgroup of V. Set $F = F'V_1$ and $E = (C \cap V)^c \cdot E'$, where $(C \cap V)^c$ is the connected component of the identity in $C \cap V$. Then from $G^* = \phi(MF'E)$ we deduce

$$G = MF'EV = MF'VE = MF'V_1(C \cap V)^c \cdot E = MFE.$$

To prove that $G = M \cdot F \cdot E$ topologically, it suffices to prove that

$$G = M \cdot F' \cdot V_1 \cdot (C \cap V_1)^c \cdot E'$$

topologically. Inasmuch as $V = V_1 \cdot (C \cap V)^c$ topologically, it suffices to prove $G = M \cdot F' \cdot V \cdot E'$ topologically. Let θ denote the mapping $(m, f, v, e) \to mfve$ of $M \times F' \times V \times E'$ onto G.

θ is bi-unique. For $m_1 f_1 v_1 e_1 = m_2 f_2 v_2 e_2$ (m_i in M, etc,) implies $\phi(m_1)\phi(f_1)\phi(e_1) = \phi(m_2)\phi(f_2)\phi(e_2)$. Since $M \cap V$ is a compact subgroup of V, it consists only of the identity and hence ϕ is one-to-one on M. By construction ϕ is one-to-one on F' and E'. Hence $G^* = \phi(M) \cdot \phi(F') \cdot \phi(E')$ topologically implies $\phi(m_1) = \phi(m_2)$, $\phi(f_1) = \phi(f_2)$, $\phi(e_1) = \phi(e_2)$ and consequently, $m_1 = m_2$, $f_1 = f_2$, $e_1 = e_2$. It follows that $v_1 = v_2$ and θ is bi-unique. That θ is a homeomorphism follows as in Case 1.

Case 2b. There exists a non-trivial normal analytic subgroup V with $\mathscr{C}\ell\, CV \neq G$.

Take H to be the subgroup $\mathscr{C}\ell\, CR$ if this does not coincide with G,

otherwise take it to be $\mathfrak{Gl}\,CV$. Then H, being a closed connected subgroup, is analytic and moreover, its dimension is smaller than the dimension of G.

We assert that C and H are self-adjoint modulo the radical in H and G respectively. For by hypothesis there is a star automorphism of G/R which keeps invariant CR/R and this clearly keeps invariant $\mathfrak{Gl}\,(CR/R) = (\mathfrak{Gl}\,CR)/R$. Thus the assertion is true for H if $G \neq \mathfrak{Gl}\,CR$. If, on the other hand, $G = \mathfrak{Gl}\,CR$, then by a result of Malcev (cf. first paragraph of proof of Proposition 2.1), $[G, G] \subset CR$ and thus

$$G/R = [G/R, G/R] = [G, G]R/R = CR \neq R$$

so that $\mathfrak{Gl}\,CV$ is self-adjoint modulo the radical in G in this case. Thus in any event, H is self-adjoint modulo the radical in G.

As for C being self-adjoint modulo the radical in H, the star automorphism of G which keeps H invariant induces a star automorphism of H/S which keeps invariant CS/S, S denoting the radical of H. Thus C is self-adjoint modulo the radical in H.

Applying the induction assumption to the pair C, H, we obtain $C = M_C \cdot E$ and $H = M_H \cdot F_1 \cdot E$ topologically, where M_H is a maximal compact subgroup of G containing M_C, E, and F_1 and hence $F_1 \cdot E$ are M_C-invariant exp-sets.

We now apply Case 1 to the pair H, G, and conclude that $H = M_H \cdot E_1$, $G = M \cdot F_2 \cdot E_1$ where E_1 and F_2 are M_H-invariant exp-sets and M is a maximal compact subgroup of G containing M_H.

Any element y of E can be written uniquely as $y = m_1 f_1 e$ with m_1, f_1, e in M_H, F_1, E respectively and depending continuously on y. Hence any element x of G can be expressed uniquely as $x = m f_2 \cdot m_1 f_1 e = m m_1 \cdot m_1^{-1} f_2 m_1 \cdot f_1 \cdot e_1$ with the factors in M, F_2, F_1, E respectively and depending continuously on x. Hence $G = M \cdot F_2 \cdot F_1 \cdot E_1 = M \cdot F \cdot E_1$ topologically where F is the M_C-invariant exp-set $F_2 F_1$. Proof is now complete in this case.

Case 2c. $R \neq 0$ and for any non-trivial normal abelian analytic subgroup V, $G = \mathfrak{Gl}\,CV$.

In this case, there exists a normal analytic abelian non-trivial subgroup W such that $G = CW$ by Proposition 2.1 and the Note following it. Thus we may apply the result in Case 2a to obtain the theorem.

The induction hypothesis has thus been proved to hold for G in case G has a non-trivial radical. It remains only to consider

Case 3. G has no radical.

Here G is semi-simple and we can apply Theorem 5 of Section 1 in [10]

which asserts: Let $\mathfrak{K}+\mathfrak{E}$ be a Cartan decomposition for the real semi-simple Lie algebra $\mathfrak{G}$ and let $\mathfrak{E}'$ be a linear subspace of $\mathfrak{E}$ such that $[X,[X,Y]]$ is in E' for any X, Y in E'. Let $\mathfrak{F}$ be the orthogonal complement to $\mathfrak{E}'$ in $\mathfrak{E}$ with respect to the Killing form, let $F=\exp\mathfrak{F}$, $E'=\exp\mathfrak{E}'$. Then $G=K\cdot F\cdot E'$ topologically where K is the analytic subgroup determined by $\mathfrak{K}$.

In Case 3, C is self-adjoint in G and therefore there exists a Cartan decomposition $\mathfrak{K}+\mathfrak{E}$ with $\mathfrak{C}=\mathfrak{C}\cap\mathfrak{K}+\mathfrak{C}\cap\mathfrak{E}$. Set $\mathfrak{E}'=\mathfrak{C}\cap\mathfrak{E}$. Then $\mathfrak{E}'$ satisfies the hypothesis of the cited theorem and therefore $G=K\cdot F\cdot E'$ topologically, notation being as above. In addition, we have $C=(C\cap K)\cdot E'$ topologically. For the subsets $C\cap K$ and E' being closed, $(C\cap K)\cdot E'$ is a closed subset of C. On the other hand, the mapping $\theta:(c,e)\to ce$ of $(C\cap K)\times E'$ into C is one-to-one and continuous; since $(C\cap K)\times E'$ is locally Euclidean and of the same dimension as C, the mapping θ is open by the theorem on the invariance of domain. As a result, $(C\cap K)\cdot E'$ is open and closed in the connected group C and hence coincides with C. Inasmuch as $\mathfrak{E}$ is invariant under $\operatorname{ad}\mathfrak{K}$ we conclude that E' and F' are $(C\cap K)$-invariant exp-sets.

The choice of F and E is not yet complete inasmuch as K need not be compact. We know only that the image of K in the adjoint group of G is compact. This implies that the adjoint groups of K and $C\cap K$ are compact. It follows at once that each is the direct product of its maximum compact subgroup and a vector group (cf. [9], Lemma 2.8). Let M_1 be the maximum compact subgroup of C and let W be a vector subgroup such that $C=M_1\cdot W_1$ (direct). Let W_2 be a vector subgroup of K such that $K=(MC)\cdot W_2$ (direct) where M is the maximum compact subgroup of K. Set $E=W_1E'$ and $F=W_2F''$. Since $W_1\subset C\cap K$, $W_2\cdot F'=F'\cdot W_2$, we get

$$\begin{aligned}G&=M\cdot W_1\cdot W_2\cdot F''\cdot E'=M\cdot W_2\cdot W_1\cdot F''\cdot E'\\&=M\cdot W_2\cdot F''\cdot W_1\cdot E'=M\cdot F\cdot E \text{ topologically.}\end{aligned}$$

Finally, M_1 is a maximum compact subgroup of C. For let M_C be a maximal compact subgroup of C which contains M_1. Since $C=M_1\cdot E$ topologically, G/M_1 is homeomorphic to Euclidean space and it is fibered by the compact fibers M_C/M_1 with $G/M_1/M_C/M_1=G/M_C$ as base space. Since Euclidean space cannot be fibered by compact fibers containing more than one point ([2] or [12]), we conclude that $M_1=M_C$. Proof of the theorem is now complete.

Note. The theorem from [10] that was cited in Case 3 arises out of the following theorem, which the author proved with precisely the above application in mind.

Let $\mathfrak{E}$ be any real linear subspace of $\mathfrak{S}$, the set of real symmetric matrices, and let $\mathfrak{F}$ be an orthogonal complement to $\mathfrak{E}$ in $\mathfrak{S}$ with respect to the bilinear form $\operatorname{Tr} XY$. Then any positive definite symmetric matrix can be written uniquely and continuously as efe with e in $\exp \mathfrak{E}$ and f in $\exp \mathfrak{F}$, if and only if $[\mathfrak{E}, [\mathfrak{E}, \mathfrak{E}]] \subset \mathfrak{E}$.

When we specialize the choice of C to a maximal compact subgroup M, we obtain the following sharpened form of the theorem on the topological decomposition of a Lie group.

THEOREM 2.2. *Let G be a connected Lie group and let M be a maximal compact subgroup of G. Then $G = M \cdot U$ topologically, where U is an M-invariant exp-set.*

In particular, U is a Euclidean subspace with $mUm^{-1} = U$ for all m in M, and M operating on U by inner automorphisms is equivalent to the linear group $\operatorname{Ad} M$ operating on a linear subspace of G.

Theorem 2.2 allows us to sharpen the theorem on the conjugacy of maxima[1] compact subgroups of connected Lie groups.

Remark. That any two maximal compact subgroups of a connected Lie group G are conjugate under inner automorphisms has been proved by Malcev ([7]) and Iwasawa ([6]). Each proof takes as starting point the theorem of E. Cartan that maximal compact subgroups of a semi-simple group are conjugate (cf. [3] or [10]). It is of interest to observe that the idea introduced by Cartan to handle the semi-simple case can be used to handle the general case. We sketch the argument. Proceeding by induction in the case that G is not semi-simple, we reduce to the case that G contain a non-trivial closed normal vector subgroup V (cf. proof of Theorem 2.1).

Applying the induction assumption to G/V, it follows that if M_1 and M_2 are maximal compact subgroups, then M_2 is conjugate under an inner automorphism to a subgroup of M_1V. Hence we lose no generality in assuming that $M_2 \subset M_1V = G$, with G connected. M being compact, $M_1 \cap V =$ (identity) so that $G = M_1 \cdot V$ topologically. Hence $G/M_1 = V$. Now upon selecting logarithmic coordinates in V, it is seen that G operating on V is equivalent to group of affine transformations, the elements of V operating as translations. Hence any compact subgroup of G admits a fixed point in V, the centroid of any of its orbits. Thus there is an element x in G such that M_2xM_1 is simply the coset xM_1; that is, $M_2xM_1 \subset xM_1$ and $x^{-1}M_2x \subset M_1$. Thus M_1 and M_2 are conjugate. That M_1 is connected follows from the connectedness of G.

THEOREM 2.3′. *Let M_1 and M_2 be any two maximal compact subgroups*

of the connected Lie group G. Then there is an element x in G such that $xM_1x^{-1} = M_2$ and $xmx^{-1} = m$ for all m in $M_1 \cap M_2$.

Proof. We begin with the fact that any two maximal compact subgroups of G are conjugate under an inner automorphism. Thus we may assume that M_1 is the subgroup M of Theorem 2.2, i.e., there is a subspace U such that $G = M_1 \cdot U$ topologically and $mUm^{-1} = U$ for all m in M. We know there is an element y in G such that $yM_1y^{-1} = M_2$. Now y can be written as xn with n in M, and x in U. Then $xM_1x^{-1} = xnM_1n^{-1}x^{-1} = yM_1y^{-1} = M_2$. Thus $xM_1x^{-1} = M_2$ and hence $x(M_1 \cap M_2)x^{-1} \subset M_1$. For any element m in $M_1 \cap M_2$ we have the relation $xmx^{-1} \cdot x = xm = m \cdot m^{-1}xm$.

Since $xmx^{-1} \in M_1$, $m^{-1} \in U$, and $G = M_1U$ topologically, we infer $xmx^{-1} = m$, which proves the theorem.

More generally, we can assert

THEOREM 2.3. *Let N_1 and N_2 be two compact subgroups of the connected Lie group G which are conjugate under an inner automorphism θ_1. Let M_1 and M_2 be any maximal compact subgroups which include N_1 and N_2 respectively. Then there exists an inner automorphism θ of G which sends M_1 onto M_2 and which coincides with θ_1 on N_1.*

Proof. Let $M_3 = \theta_1(M_1)$. Applying Theorem 2.3′ to M_3 and M_2, we find an inner automorphism θ_2 sending M_3 into M_2 and keeping $M_3 \cap M_2$ pointwise fixed. The inner automorphism $\theta = \theta_2\theta_1$ has the desired properties.

3. Retraction of Klein spaces. Throughout this section, G denotes a connected closed subgroup, and M any maximal compact subgroup of G which includes a maximal compact subgroup of C.

THEOREM 3.1. *G/C can be retracted by a strong deformation retraction to a subset homeomorphic to the h-compact space $M/M \cap C$. Thus G/C and $M/M \cap C$ have the same homotopy type.*

Proof. For convenience, let M_C denote $M \cap C$. By hypothesis M_C is a maximal compact subgroup of C. By Theorem 2.2, C/M_C is topologicaly a Euclidean space and is thus solid (cf. [13] for definition). Moreover, G/M_C is a fiber bundle with G/C as base space and C/M_C as fiber, the projection p being $[xM_C] \to [xC]$, (x in G).

Let ϕ denote the mapping $[xC] \to [xM_C]$ for x in M. Since $M \cap C = M_C$, ϕ is well-defined and is a continuous cross-section of the subset MC/C of G/C into the bundle G/M_C. Since the fiber C/M_C is solid, ϕ can be extended to a continuous cross-section of G/C into G/M_C ([13]). We denote this extension

by ϕ also. From the fact that $G = U \cdot M$ topologically with U a Euclidean subspace, it follows at once that there is a strong deformation retraction $S_t (0 \leqq t \leqq 1)$ of G/M_C onto the subset M/M_C (the points of M/M_C being fixed under the deformation). We define the retraction R_t of $G_C C$ onto itself as $R_t = pS_t\phi (0 \leqq t \leqq 1)$. Then for any x in M,

$$R_t([xC]) = pS_t([xM_C]) = p([xM_C]) = [xC].$$

Moreover, $R_0 =$ identity, and $R_1(G/C) = MC/C = M/M \cap C$. Thus R_t is the desired strong deformation retraction of G/C.

COROLLARY 1. *If S is a closed subgroup of G and G/S is simply connected, then the conclusion of the above theorem holds.*

Proof. If G/S is simply connected, then S is connected.

COROLLARY 2. (Montgomery, [8]). *If G is a Lie group that is transitive on a simply connected compact space, then there is a compact subgroup of G that is transitive on the space. Thus every simply connected compact Klein space is h-compact.*

Proof. We may assume that our space is G/C where C is connected, and G/C is a compact manifold. Since a compact manifold cannot be deformed to a proper subset, $G/C = MC/M$, i.e., M is transitive on G/C and $G/C = M/M \cap C$.

4. Covariant fiberings. Let B be a Lie group, B' a closed subgroup of B, let F denote a topological space, and let λ denote an anti-homomorphism of B' into the group of all homeomorphisms of F onto itself (cf. [0]). Assume that B operates on F as a topological transformation group in the usual sense, i.e., the mapping $(g, f) \to \lambda(g)f$ of $B' \times F$ into F is continuous. We define the subset $[b, f]$ for any point (b, f) in $B \times F$ as $\{(bg, \lambda(g)f) \mid \text{all } g \in B'\}$. If U is a subset of $B \times F$, we denote by $[U]$ the set $\{[b, f] \mid (b, f) \in U\}$.

Definition. (B, F, B', λ) denotes the topological space whose points are the subsets $[b, f]$ *of* $B \times F$, a neighborhood of $[b, f]$ being defined as $[U]$ where U is any neighborhood of (b, f) *in* $B \times F$.

Let π denote the mapping $(b, f) \to [b, f]$ of $B \times F$ onto (B, F, B', λ). Then by definition essentially, π is continuous and open. (B, F, B', λ) can be thought of as the space obtained from $B \times F$ by taking as points the (non-singular) orbits of the transformation group $R(B')$, where $R(g)$ is the mapping $(b, f) \to (bg, \lambda(g)f)$, $b \in B$, $g \in B'$, $f \in F$.

We next define on (B, F, B', λ) a fiber bundle structure, with base space B/B', fiber F, and as structure group the Lie group $\lambda(B')$. Namely, let p be the mapping $[b, f] \to bB'$ of (B, F, B', λ) onto B/B'. Let $U_1, \cdots, U_i, \cdots$ be a covering of B/B' by neighborhoods such that there exists a continuous cross-section ψ_i of U_i into the bundle B fibered by cosets B' (b in B). Define $\phi_i : p^{-1}(U_i) \to U_i \times F$ by the relation $\phi_i(\psi_i(x), f) = (x, f)$, ($x$ in U_i, f in F). It is easily seen that ϕ_i constitutes a set of coordinate functions which defines (B, F, B', λ) as a bundle with fiber F and structure group $\lambda(B')$. We shall employ the symbol (B, F, B', λ) to denote the above bundle structure as well as the underlying space, when there is no danger of confusion. It is clear from the choice of coordinate functions that the associate principal bundle of (B, F, B', λ) is the bundle B fibered by cosets bB'.

Definition. Suppose B and F are closed subsets of a prescribed Lie group G. Suppose moreover that F is invariant under inner automorphisms by elements of B', that F contains the identity element of G, and that $\lambda(g)$ denotes the transformation $f \to g^{-1}fg$ where $f \in F$ and $g \in B'$. We then denote (B, F, B', λ) by the symbol $(B \times F)_{B'}$.

Let (B, F, B', λ) be given. If the group of transformations $\lambda(B)$ has a fixed point p_0 in F, then the mapping $[bB'] \to [b, p_0]$ of B/B' into (B, F, B', λ) is well defined and is in fact a continuous cross-section of the base space B/B' into the fiber bundle (B, F, B', λ). In particular, the mapping $[bB'] \to [b, e]$ of B/B' into $(B \times F)_{B'}$ is a continuous cross-section, where e is the identity of the prescribed group G.

LEMMA 4.1. *Let G be a Lie group, let C and B be closed subgroups, and let F, E be two subspaces of G such that, $G = B \cdot F \cdot E$ (topologically). Assume*

(1) *$C = B' \cdot E$ (topologically) where B' is a subgroup of B.*

(2) *$g^{-1}Fg$ F for all $g \in B'$.*

(3) *F contains the identity element of G.*

Then $G/C = (B \times F)_{B'}$ under the homeomorphism $[bfC] \to [b, f]$.

Proof. Let θ denote the mapping $(b, f) \to bfC$ of $B \times F$ onto G/C. For each point of G/C, $\theta^{-1}[bfC]$ is the totality of pairs (b^*, f^*) in $B \times F$ such that $b^*f^* = bfC = bfge = bg \cdot g^{-1}fg \cdot e$ with $c \in C$, $g \in B'$, $e \in F$. Hence $b^* = bg$, $f = g^{-1}fg$, and so $\theta^{-1}[bfC]$ is the subset $[b, f] \subset B \times F$. As a result, the correspondence $\pi\theta^{-1} : \theta(b, f) \to (b, f)$ is a well defined one-to-one correspondence between G/C and $(B \times F)_{B'}$. Since both θ and π are open and continuous mappings, $\pi\theta^{-1}$ is a homeomorphism. Proof of the lemma is now complete.

Remark 4.1. Suppose that $G = B \cdot F \cdot E$ topologically and $C = B' \cdot E$ topologically, with B' a subgroup of B as above. Assume moreover that $bFb^{-1} \subset F$ for all b in B. Then G is also $F \cdot B \cdot E$ topologically. From these two decompositions of G we obtain two different fiber bundles (in general) which are associated with the *same* fibering of G/C into the subsets bF $(= Fb)$ with b in B; the bundles are (B, B', F, λ_1) and (B, B', F, λ_2) respectively, where λ_1 corresponds to the operation of B' on F by inner automorphisms, and $\lambda_2(B')$ is the identity transformation. The bundle $(B, B', F, \lambda_1) = (B \times F)_{B'}$ has as structure group $\lambda_1(B')$ and the other has as structure group $\lambda_2(B)$ = (identity), these groups being different in general. Since these correspond to the same fibering of G/C, they are equivalent when the structure group of each bundle is suitably augmented.

Remark 4.2. The group B operates on (B, B', F, λ) by the operations $L_b^* : [xf] \to [bx, f]$, where b, x are in B and f is in F. L_b^* is a well defined bundle map of (B, B', F, λ) onto itself, and L_B^* permutes the fibers transitively.

In the special case that $(B, B', F, \lambda) = (B \times F)_{B'}$, and the subsets B and F of G are as in Lemma 4.1, the operation L_B^* is the operation of B on G/C by left translation. In this case, the operation $R(b) : (x, f) \to (xb, b^{-1}xb)$ with b in B' corresponds to the operation of b on BF by right translation.

Definition. Let G be a connected Lie group which operates transitively on the space H. A *G-covariant fibering* of the differentiable manifold H is a differentiable fibering into Euclidean fibers (i.e., the fibers are submanifolds and each fiber has as neighborhood an open set of fibers with a differentiable submanifold as cross-section set) such that for some maximal compact subgroup M of G,

1) M permutes the fibers transitively.

2) For some fiber F, the subgroup M_F of M which keeps F invariant is equivalent to a group of linear transformations on the Euclidean space F.

Condition 2) is obviously equivalent to the condition obtained on replacing "some fiber F" by "each fiber F," in view of the fact that M permutes the fibers transitively.

THEOREM 4.1. *Let G be a connected Lie group which operates transitively on the space H with a connected isotropy subgroup C. Assume that C is self-adjoint modulo the radical. Then H admits a G-covariant fibering.*

Proof. By Theorem 2.1, $G = M \cdot F \cdot E$ topologically, where M is a maximal compact subgroup, $C = M_C \cdot E$ topologically, with $M_C = M \cap C$, and

F is an M_C-invariant exp-set. By Lemma 4.1, $H = G/C$ is the underlying space of the fiber bundle $(M \times F)_{M_C}$. Since M permutes the fibers of this bundle transitively (Remark 4.2), F is Euclidean. To conclude the proof of our theorem it suffices to verify that a) M_F, the subgroup of M keeping the fiber F invariant is equivalent to a linear group, and b) $(M \times F)_{M_C}$ is a differentiable fibering of H. Part a) follows from the observation that $M_F = M_C$ and M_C operating on F is equivalent to the linear group $\mathrm{Ad}\, M_C$ operating on a linear subspace of G by definition of F. Part b) follows from the fact that decomposition $G = M \cdot F \cdot E$ is differentiable around the identity element at least, as can be verified without difficulty.

COROLLARY 1. *If C is a closed connected semi-simple subgroup of the connected Lie group G, then G/C admits a G-covariant fibering.*

Proof. Let R be the radical of G. Then CR/R is a semi-simple subgroup of the semi-simple group G/R and is self-adjoint by Theorem 6 of [10].

COROLLARY 2. *If C is a closed connected subgroup of the connected solvable Lie group G, then G/C admits a G-covariant fibering.*

Proof. G is its radical and CG/G is self-adjoint in G/G.

COROLLARY 3. *If C is a compact connected subgroup, then G/C admits a G-covariant direct product fibering.*

Proof. This follows directly from Theorem 2.2 applied to a maximal compact subgroup containing C. (cf. Remark 4.1).

Remark 4.3. The decomposition of a semi-simple Lie group G without center into $K \cdot S$ where K is a maximal compact subgroup and S is a subgroup homeomorphic to Euclidean space (due to Iwasawa [6]) allows one to conclude that G/K has a covariant fibering but does *not* allow this conclusion for G/K' when $K' \subset K$, inasmuch as S is not invariant under inner automorphisms from K'.

5. Examples. We will now consider some cases where the fiberings of Section 4 turn out to be direct product fiberings when the group of the bundle is suitably enlarged.

Definition. Let F be a locally compact Hausdorff space. By $\mathrm{aut}\, F$ is meant the group of homeomorphisms of F onto itself topologized so as to be a topological transformation group operating on F. (cf. [0], Arens).

In the case that F is Euclidean space, the compact open topology satisfies the above condition.

Conditions that the fibering of Section 4 be product fiberings can be stated most simply in terms of mappings into aut F.

We consider first the fibering defined for the space $(B \times F)_{B'}$ and employ the notation of Section 4. In particular, $\lambda(g)$ denotes the homeomorphism $f \to g^{-1}fg$ for $f \in F$, $g \in B'$. Since $\lambda(g_1g_2) = \lambda(g_2)\lambda(g_1)$, λ is an anti-homomorphism of B' into aut F.

THEOREM 5.1. *The fibering of $(B \times F)_{B'}$ is a direct product decomposition if and only if there is a continuous mapping $u: B \to \text{aut } F$ such that $u(x) = u(xg)\lambda(g)$ for each g in B'.*

Proof. If the fibering is a direct product decomposition, then there exists a fiber-preserving homeomorphism ϕ of $(B/B) \times F$ onto $(B \times F)_{B'}$ such that $\phi([xB'], _1) = (x, f)$ $(= (xg, g^{-1}fg) = (xg, \lambda(g)f)$ for g in $B')$. Define $u(x)$ to be the mapping $f \to f_1$ of F onto F, where $x \in B$. Since ϕ is a fiber preserving homeomorphism, $u(x)$ is a homeomorphism. Moreover u is a continuous mapping of B into aut F. Finally, since (x, f) and $(xg, \lambda(g)f)$, g in B', represent the same point of $(B \times F)_{B'}$, we have the identity $u(x)(f) = u(xg)(\lambda(g)f)$ for any f in F, i.e., $u(x) = u(xg)\lambda(g)$ for all g in B'.

Conversely, suppose there is such a mapping u. Then consider the mapping $\theta: (x, f) \to ([xB'], u(x)f)$ of $B \times F$ into $(B/B') \times F$. The mapping θ is single-valued, open and continuous. Thus θ is a fiber preserving homeomorphism of $(B \times F)_{B'}$ with $(B/B') \times F$.

Let $\mathfrak{R}$ and $\mathfrak{C}$ denote the field of real complex numbers respectively.

We employ the notation $Sl(n, \mathfrak{R})$, $Sl(n, \mathfrak{C})$, $SO(n, \mathfrak{R})$, $SO(n, \mathfrak{C})$, $SU(n)$ to denote the linear groups over real and complex numbers of determinant 1, the orthogonal groups over $\mathfrak{R}$ and $\mathfrak{C}$ of determinant 1, and the unitary group of determinant 1.

Example 1. We examine the fibering of the space G/C, where G is the group of matrices $Sl(n+1, \mathfrak{R})$ and C is the subgroup $Sl(n, \mathfrak{R})$ of the form $\begin{pmatrix} 1 & 0 \\ 0 & g \end{pmatrix}$, g being an n by n matrix. Let $\mathfrak{N}$ and $\mathfrak{S}$ denote the totality of skew-symmetric and symmetric matrices, respectively. Let $\mathfrak{E} = \mathfrak{C} \cap \mathfrak{S}$ and define $\mathfrak{F} = \{X \mid X \in \mathfrak{S}, \text{Tr } XY = 0 \text{ for all } Y \in E\}$. Then $\mathfrak{F}$ is the totality of symmetric matrices (s_{ij}) with $s_{ij} = 0$ if $i > 1$ and $j > 1$. We set $\mathfrak{N}' = \mathfrak{C} \cap \mathfrak{N}$, $\mathfrak{F} = \exp \mathfrak{F}$. We define $\lambda(g)$ to be the mapping $f \to g^{-1}fg$ in aut F, where g is in the analytic subgroup K'. Let $A(g)$ denote the restriction of Ad g to $\mathfrak{F}$ where $g \in K'$. Let log denote the homeomorphism $\exp X \to X$ of F onto $\mathfrak{F}$. Since $\lambda(g)(\exp X) = \exp(\text{Ad } g^{-1}(X))$ for all $X \in \mathfrak{F}$, $g \in K'$, we have

$\log \cdot \lambda(g) = A(g^{-1}) \cdot \log$, that is, the homeomorphism log is equivalent with respect to the isomorphism $\lambda(g) \to A(g^{-1})$. We now look at the transformation group $A(K')$. If $X \in \mathfrak{F}$, then

$$X = \begin{pmatrix} a & b' \\ b & c \end{pmatrix}, \qquad c = -a/n \cdot (\text{identity})$$

and

$$A(g)X = \begin{pmatrix} 1 & 0 \\ 0 & g \end{pmatrix}\begin{pmatrix} a & b' \\ b & c \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & g \end{pmatrix}^{-1} = \begin{pmatrix} a & b'g^{-1} \\ gb & c \end{pmatrix}, g \in K'.$$

This identity has the following interpretation. Let ϵ_i denote the $(n+1)$-tuple with components δ_{ij} $(i, j = 1, \cdots, n+1)$. Let X_i denote the matrix of F whose p, q-th coefficient is $\max_i \{\delta_{ip}\delta_{iq}, \delta_{iq}\delta_{ip}\}$. Let ϕ denote the unique linear mapping of F onto the Cartesian space $\mathfrak{R}^{n+1}$ (on which $G = Sl(n+1, \mathfrak{R})$ operates) such that $\phi(X_i) = \epsilon_i$ $(i = 1, \cdots, n+1)$. The above identity states that $g\phi = \phi A(g)$, $g \in K' = SO(n, R)$, that is, the homeomorphism ϕ is equivariant with respect to the isomorphism $A(g) \to g$ of $A(K')$ onto K'.

Now define $u(x) = (\phi \log)^{-1} x \phi \log$ for $x \in K = SO(n+1, R)$. Then u is a homeomorphism (in fact, an isomorphism) of K into aut F. Furthermore, $u(g) = \log^{-1} \cdot \phi^{-1} \cdot g \cdot \phi \cdot \log = \log^{-1} A(g) \log = \lambda(g^{-1})$, $g \in K'$. Thus $u(xg)\lambda(g) = u(x)u(g)u(g^{-1}) = u(x)$ for all $g \in K'$.

It follows now from Theorem 5.1 that $G/C = (K \times F)_K = K/K' \times F$. Thus $Sl(n+1, \mathfrak{R})/Sl(n, \mathfrak{R})$ decomposes, by the covariant fibering of Section 4, into the direct product of an n-sphere and a Euclidean space.

Example 2. By the same reasoning one can prove that

$$Sl(n+1, \mathfrak{C})/Sl(n, \mathfrak{C}) \; (SU(n+1)/SU(n)) \times \textit{Euclidean space}.$$

These results can be obtained by an elementary geometric argument upon representing elements of our group as a base for $\mathfrak{R}^{n+1}$ (or $\mathfrak{C}^{n+1}$ as the case may be).

Example 3. If $G = Sl(3, \mathfrak{C})$ and C is the subgroup $Sl(3, R)$, then G/C is the space of a fiber bundle with base $SU(3)/SO(3, \mathfrak{R})$ and a three dimensional Euclidean space F as fiber. The covariant fibering of G/C is not a direct product decomposition. For let us select the Cartan decomposition of $\mathfrak{G}$ (regarded as a real Lie algebra, cf. Section 2) with the maximal subalgebra $\mathfrak{K}$ taken to be the Lie subalgebra of $SU(3)$. Then K, K' are $SU(3)$, $SO(3, \mathfrak{R})$ respectively, and $\lambda(K')$ is equivalent to K' operating on real cartesian space $\mathfrak{R}^3$. The existence of a mapping u of Theorem 5.1 is equivalent to the existence of a continuous mapping u of $SU(3)$ into aut $\mathfrak{R}^3$ such that

$u(xg)g^{-1} = u(x)$, i.e., $u(xg) = u(x)g$ for all x in $SU(3)$, g in $SO(3, \mathcal{R})$. But such a mapping cannot exist. For if it did, u^{-1}(identity) would be a continuous cross-section of cosets of $SO(3, R)$ in $SU(3)$. This implies that $SU(3) = (SU(3)/SO(3, \mathcal{R})) \times SO(3, \mathcal{R})$. But comparing homotopy groups, $\pi_4(SU(3)) = 0$, whereas $\pi_4(SO(3)) \neq 0$ ([13]). Thus $SO(3, R)$ cannot be a direct factor of $SU(3)$ and the given fibering of $Sl(3, \mathcal{C})/Sl(3, \mathcal{R})$ is not a product fibering. It should be noted that the isotropy subgroup in this example is connected and *semi-simple*; also the group G is semi-simple.

Example 4. Samelson's example of a Klein space with connected isotropy subgroup but no direct product fibering can be described as follows. Take G to be the subgroup of $Sl(n+1, C)$ whose first column has only zeros below the first row. Let C be the subgroup of G whose coefficients in the second column outside of the $(2, 2)$ term consists of zeros. Clearly G and C are connected. G (resp. C) can be identified with the subgroup of projective transformations of the complex projective plane P^n, which keeps a point (resp. two points) invariant. Hence G/C can be identified with the exterior of a point p_0 in P^n. If $P^n - p_0$ could be factored into a direct product of a compact subset and a Euclidean subspace, we would be able to deform P_∞, the plane at infinity, into a singular cycle which fails to intersect P_∞, contrary to the fact that the singular cycle P_∞ has a non-zero self-intersection. Thus G/C has no direct product fibering. It has, however, a G-covariant fibering. It is noteworthy that G/CR admits a direct product covariant fibering, R being the radical of G. Thus the radical of G plays an essential role in Samelson's example.

Example 5. Let G^* be the connected component of the identity of the Lie group leaving $x_1^2 + x_2^2 + \cdots + x_n^2 - x_{n+1}^2 - x_{n+2}^2$ invariant. Let C^* be the analytic subgroup keeping invariant $x_1^2 + \cdots + x_n^2 - x_{n+1}^2$ together with x_{n+2}. Clearly, G^* and C^* are semi-simple; under the natural imbedding, $SO(n) \times SO(2)$ and $SO(n)$ are maximal compact in G^* and C^* respectively. Let G denote the simply connected covering group of G^*, and let C denote the analytic subgroup corresponding to C^*. Since $G^* = SO(n) \times SO(2) \times$ Euclidean space, the analytic subgroup M in G which covers $SO(n)$ is maximal compact in both G and C. By Theorem 4.1, G/C admits a G-covariant fibering with base space M/M. Hence G/C is homeomorphic to Euclidean space.

Note. The above example was kindly suggested to the author by A. Borel, as an instance of the phenomenon mentioned in the footnotes in Section 6.

6. Aspherical Klein spaces. As an application of Theorem 2.1, we prove

THEOREM 6.1. *An aspherical (in dimensions* $0, 1, 2, \cdots$*) Klein space is homeomorphic to Euclidean space.*

Proof. A Klein space is a factor space G/C with G a Lie group and C a closed subgroup. We shall prove the theorem for aspherical factor spaces G/C by induction on the pair of integers $(\dim G, \dim G - \dim C)$ ordered lexicographically. It is convenient to break up the proof into a series of lemmas.

LEMMA 6.1. *Let $\tilde{G}$ denote the universal covering group of the connected component G_0 of the Lie group G, and let $\tilde{C}$ be the complete inverse image in $\tilde{G}$ of $C \cap G_0$. Assume G/C is aspherical. Then $\tilde{G}/\tilde{C} = G/C$. $\tilde{C}$ is connected and contains a maximal compact subgroup of G.*

Proof. G_0 is a closed normal subgroup of G and G/G_0 is discrete. As a result, G_0C is an open and closed subset of G and G_0C/C is open and closed in G/C. Since G/C is connected, $G_0C/C = G/C$ and therefore

$$\tilde{G}/\tilde{C} = G_0/C \cap G_0 = G_0C/C = G/C.$$

Since $\tilde{G}/\tilde{C}$ is simply connected, $\tilde{C}$ is connected. Let K be any maximal compact subgroup of $\tilde{G}$ which includes a maximal compact subgroup of $\tilde{C}$. By Theorem 3.1, $\tilde{G}/\tilde{C}$ has the same homotopy type as $K/K \cap \tilde{C}$. Since the homotopy groups of all dimensions of $K/K \cap \tilde{C}$ vanish, by the well known theorem of Hurewicz, all the positive dimension homology groups with integral coefficients of $K/K \cap \tilde{C}$ vanish. However, $K/K \cap \tilde{C}$, being a simply connected manifold, is orientable and hence it has a fundamental cycle which is not homologous to zero. It follows immediately that $K/K \cap \tilde{C}$ is a 0-dimensional manifold and being connected, it is a point. Thus $K = K \cap \tilde{C}$. Proof of the lemma is now complete.

LEMMA 6.2. *Let G be a Lie group, and let B, C be closed subgroups with $B \supset C$. If G/B and B/C are Euclidean (spaces topologically), then G/C is Euclidean.*

Proof. G/C can be considered as a fiber bundle over the case space G/B with fibers B/C, the projection being $p: [xC] \to [xB]$ and the group of the bundle being the group of left translations of the space of cosets B/C by elements of B. It is known that there always exists a continuous cross-section of a base space into a fiber bundle in case the base space is Euclidean

(Feldbau [5]). In particular, there is a continuous cross-section of G/B into the principal bundle of the bundle G/C. Consequently, the above bundle G/C is the product bundle $G/B \times B/C$. Thus G/C is Euclidean.

LEMMA 6.3. *A maximal proper analytic subgroup (i.e., connected Lie subgroup) of a simply connected Lie group is closed.*

Proof. Let G be the simply connected Lie group and C a maximal proper analytic subgroup. If C is not closed then $\overline{C} = G$ and the Lie algebra $\mathfrak{C}$ of C is an ideal in $\mathfrak{G}$ (cf. Section 2; also [7]). Hence C is normal in G and consequently is closed (Pontriagin, *Topological Groups*, p. 279).

LEMMA 6.4. *Let G be a simply connected simple real Lie group, Let C be a closed connected subgroup of G, and let M be a maximal compact subgroup of G. Assume $C \supset M$. Then G/C is homeomorphic to Euclidean space.*

Proof. Let $\mathfrak{G}$, $\mathfrak{C}$, $\mathfrak{M}$ denote the Lie algebras of G, C, M, respectively. Let $\mathfrak{K} + \mathfrak{E}$ be a Cartan decomposition for the simple Lie algebra $\mathfrak{G}$ (Section 2). Since all maximal compace subgroups of a connected semi-simple Lie group are conjugate and K contains a maximal compact subgroup of G, we may assume that $\mathfrak{M} \supset \mathfrak{K}$ and then $\mathfrak{K} = \mathfrak{M} + \mathfrak{A}$ (direct algebraically) where $\mathfrak{A}$ is abelian and $\mathfrak{M}$ is semi-simple or (0) (cf. [9]). Furthermore, since $\mathfrak{G}$ is simple, $\operatorname{ad}\mathfrak{K}$ is irreducible on $\mathfrak{E}$ (cf. [3]).[2] As a result, the center of $\mathfrak{K}$ is at most one-dimensional. In particular, $\dim \mathfrak{M}$ is 0 or 1.

We must now distinguish in our argument between the cases $\mathfrak{M} = 0$ and $\mathfrak{M} \neq 0$. If $\mathfrak{M} = 0$, then G is of rank 1, dimension 3, and not compact. In this case, $\mathfrak{G}$ is isomorphic to the Lie algebra of all 2×2 real matrices with trace zero, and we identify $\mathfrak{K}$ and $\mathfrak{E}$ with the skew-symmetric, and symmetric matrices of trace 0 respectively. In this case, it is well known that a one-dimensional subalgebra $\mathfrak{C}$ is conjugate under an inner automorphism to either $\mathfrak{K}$ or a subalgebra of triangular matrices. Hence we can assume if $\dim \mathfrak{C} = 1$ that either $\mathfrak{C} = \mathfrak{K}$ or $\mathfrak{C}$ is a subalgebra of triangular matrices. In either case, G/C is homeomorphic to Euclidean space. If $\dim \mathfrak{C} = 2$, then as is known, $\mathfrak{C}$ is conjugate to the subalgebra of triangular matrices and $G/C \cap K =$ Euclidean space. (Alternatively, G/C being a one-dimensional simply connected separable space, is Euclidean).

Thus we need only consider the case $\mathfrak{M} \neq 0$. Here, the center of $\mathfrak{K}$ can be described as the centralizer of $\mathfrak{M}$ in $\mathfrak{G}$. For let $\mathfrak{N}$ denote the normalizer $\mathfrak{M}$ in $\mathfrak{G}$, i.e., $N = \{X \mid X \in \mathfrak{G}, [X, \mathfrak{M}] \subset \mathfrak{M}\}$. Since $\mathfrak{K} \subset \mathfrak{N}$, $\mathfrak{N} = \mathfrak{K} + (\mathfrak{N} \cap \mathfrak{E})$.

[2] However, $\operatorname{ad}\mathfrak{M}$ need not be irreducible on $\mathfrak{E}$; in fact, there may exist proper subalgebras of $\mathfrak{G}$ other than $\mathfrak{K}$ which include $\mathfrak{M}$, (cf. Example 5 of Section 5).

Since $\mathfrak{N}$ is a subalgebra and $\mathfrak{E}$ is invariant under $\operatorname{ad}\mathfrak{K}$, $\mathfrak{N}\cap\mathfrak{E}$ is invariant under $\operatorname{ad}\mathfrak{K}$. Since $\operatorname{ad}\mathfrak{K}$ is irreducible on $\mathfrak{E}$, $\mathfrak{N}\cap\mathfrak{E}=(0)$ or $\mathfrak{E}$. Thus $\mathfrak{N}=\mathfrak{K}$ or $\mathfrak{N}=\mathfrak{G}$. Since $\mathfrak{G}$ is simple, $\mathfrak{N}=\mathfrak{G}$ implies $\mathfrak{K}=\mathfrak{G}=\mathfrak{N}$. Hence in any case, $\mathfrak{N}=\mathfrak{K}$. Since the centralizer of $\mathfrak{M}$ is in $\mathfrak{N}$, it is in $\mathfrak{K}$ and is central in $\mathfrak{K}$. Conversely, the center of $\mathfrak{K}$ obviously centralizes $\mathfrak{M}$. Thus the center of $\mathfrak{K}$ is the centralizer of $\mathfrak{M}$ in $\mathfrak{G}$, which is of course $\mathfrak{A}$.

We now take up the analysis of the subalgebra $\mathfrak{C}$ under the assumption $\mathfrak{M}\neq(0)$. Inasmuch as $\mathfrak{C}\supset\mathfrak{M}$, $\mathfrak{C}=\mathfrak{M}+(\mathfrak{C}\cap(\mathfrak{A}+\mathfrak{E}))$. Now $\mathfrak{C}$, $\mathfrak{A}$ and $\mathfrak{E}$ being invariant under the completely reducible set of endomorphisms $\operatorname{ad}\mathfrak{M}$, $\mathfrak{C}\cap\mathfrak{E}$ is a subspace of $\mathfrak{C}\cap(\mathfrak{A}+\mathfrak{E})$ invariant under $\operatorname{ad}\mathfrak{M}$. Hence, $\mathfrak{C}\cap(\mathfrak{A}+\mathfrak{E})=(\mathfrak{C}\cap\mathfrak{E})+\mathfrak{A}'$, where $\mathfrak{A}'$ is invariant under $\operatorname{ad}\mathfrak{M}$. Since $\dim\mathfrak{A}\leqq 1$, we infer $\dim\mathfrak{A}'\leqq 1$. Since any one-dimensional representation of a semi-simple algebra is the zero representation, $[\mathfrak{M},\mathfrak{A}']=0$. Thus $\mathfrak{A}'$ is in the centralizer of $\mathfrak{M}$ in $\mathfrak{G}$ and hence

$$\mathfrak{A}'\subset\mathfrak{A}\cap\mathfrak{C}\subset\mathfrak{C}\cap\mathfrak{K},\quad \mathfrak{C}\cap(\mathfrak{A}+\mathfrak{E})\subset\mathfrak{C}\cap\mathfrak{E}+\mathfrak{C}\cap\mathfrak{K},$$
$$\mathfrak{C}\subset\mathfrak{M}+\mathfrak{C}\cap(\mathfrak{A}+\mathfrak{E})\subset\mathfrak{C}\cap\mathfrak{K}+\mathfrak{C}\cap\mathfrak{E}.$$

We have proved therefore that $\mathfrak{C}=\mathfrak{C}\cap\mathfrak{K}+\mathfrak{C}\cap\mathfrak{E}$. Applying Theorem 2.1 we have that $G/C=(M\times W)_{M'}$ where $M'=C\cap M=M$, and W is Euclidean. Thus G/C is homeomorphic to the space of a fiber bundle with Euclidean fiber W and with a base space $M/M'=M/M$, which is a point. Therefore, G/C is homeomorphic to Euclidean space.

We now proceed to prove Theorem 6.1. By Lemma 6.1, we may assume that G is simply connected and that C is an analytic subgroup containing a maximal compact subgroup of G. We prove by induction on the pair of integers $(\dim G, \dim G/C)$ ordered lexicographically, that: *if G is a simply connected analytic group and C is a closed (connected) analytic subgroup which contains a maximal compact subgroup of G, then G/C is Euclidean space, topologically.*[3] This induction hypothesis is certainly true for the pair $(0,0)$. Assume it true for pairs less than $(\dim G,\dim G/C)=(r,n)$. Let G_1 be a closed proper maximal analytic subgroup of G which contains C. Inasmuch as an analytic group is topologically the direct product of a maximal compact subgroup and a Euclidean space and furthermore, all maximal compact subgroups of an analytic group are conjugate, any maximal compact subgroup of simply connected Lie group is simply connected. G_1 is thus the direct product of a simply connected compact subgroup and a

[3] This result is claimed for semi-simple groups by L. Calabi in Rend. di Mat. di Univ. di Roma, Ser. 5, vol. 7 (1952), p. 326, Cor. 2. However, his proof has a central gap and would not apply to the case in Example 5 of Section 5.

Euclidean space and is hence simply connected. We can therefore apply the induction hypothesis to G/G and G/C if G contains C properly. By Lemma 6.2, G/C is Euclidean in this case. We need only consider the case $G_1 = C$, i.e., C is a maximal closed analytic subgroup of G. By Lemma 6.3, C is a maximal proper analytic subgroup of G.

Let now $\mathfrak{N}$ be any maximal ideal of $\mathfrak{G}$ which is not $\mathfrak{G}$. CN is then an analytic subgroup containing C. Thus $G = CN$ or $CN = C$. If $G = CN$, then $G/C = N/N \cap C$. By Lemma 6.1, we may assume that N and $N \cap C$ fulfill the hypotheses of our induction hypotheses (as a matter of fact, N *is* simply connected and $N \cap C$ *is* connected and contains a maximal compact subgroup of N). By our induction hypothesis $N/N \cap C$ is Euclidean, and thus G/C is Euclidean if $CN = G$.

It remains only to consider the case $CN = C$, i.e., $N \subset C$. Here $G/C = G/N/C/N$ and if $N \neq (0)$, the induction hypothesis yields the result that G/C is Euclidean. We are reduced to considering the case $\mathfrak{N} = 0$, i.e., the only ideals of $\mathfrak{G}$ are $\mathfrak{G}$ and (0). Thus G is either isomorphic to the additive group real numbers or G is a (non-abelian) simple Lie group. But by Lemma 6.4, G/C is Euclidean in this case. Our induction hypothesis has therefore been verified for the pair (r, n) and Theorem 6.1 is now proved.

7. Uniqueness of covariant fiberings. In Section 4 we defined "covariant fibering of a Klein space" and in Section 5 we saw by an example that covariant fiberings are not always trivial (i.e., direct product decompositions) even when the isotropy subgroup is connected and semi-simple. In order to understand better the significance of such an assertion, we must inquire into the uniqueness of covariant fiberings. Our concern is with the *decomposition* of the homogeneous space into fibers rather than the structure group of the fiber bundle. To that end we regard the fibered homogeneous spaces as fiber bundles whose structural group is the topological group of all homeomorphisms of the Euclidean fiber onto itself (cf. [0]).

In seeking a uniqueness theorem for covariant fiberings of a homogeneous H, we avoid the knotty problem of cofactorizations of a topological space by comparing only G-covariant fiberings. That is, we are concerned here only with fiberings that are suitably related to the operations of G on H.

Throughout this discussion, G will denote a fixed Lie group which operates transitively on a homogeneous space H. C_p will denote the isotropy subgroup of the point p in H, i.e., the subgroup of G which keeps p fixed. We assume that C_p is connected. We will consider only G-covariant fiberings of H.

Let $\mathfrak{F}$ be a fibering of H.

Definition. A *transversal* M to $\mathfrak{F}$ is a maximal compact subgroup of G which permutes the fibers of $\mathfrak{F}$. A *base point* of the transversal M is a point p whose isotropy subgroup C_p intersects M in a maximal compact subgroup of C_p. The *F-isotropy subgroup* of M is the subgroup M_F which keeps the fiber F invariant. If p is a base point of M, we call $M \cap C_p = M_p$ the *M-isotropy* subgroup of p.

We recall that a G-covariant fibering $\mathfrak{F}$ of H is a decomposition of the differential structure of H into Euclidean fibers for which there exists a transversal M with the properties:

1) The F-isotropy subgroup M_F is equivalent to a linear group on F for some fiber F.

2) M permutes the fiber transitively.

As a consequence of 2), M_F is equivalent to a linear group on F for *every* fiber F.

PROPOSITION 7.1. *Let M be a transversal of the covariant fibering $\mathfrak{F}$, and let M_F be the F-isotropy subgroup of M. Then M_F is equivalent to a linear group on the Euclidean fiber F and M permutes the fibers of $\mathfrak{F}$ transitively.*

Proof. Let G_1 be the connected component of the identity in the subgroup of G which permutes the fibers of $\mathfrak{F}$. Let G_F be the connected component of the identity in the subgroup of G_1 which keeps the fiber F invariant. Both G_1 and G_F are closed subgroups of G.

M_F is a maximal compact subgroup of G_F. For let N_F be a maximal compact subgroup of G_F which contains M_F and let N be a maximal compact subgroup of G_{11} which contains N_F. Since G_1 and G_F are connected Lie groups, there is an inner automorphism $\Gamma_g : x \to g \times g^{-1}$ with g in G, which carries M onto N and M_F into N_F (by Theorem 2.3). Since the transformation $h \to g \cdot h$ (g in G, h in H) of H onto itself is a fiber-preserving homeomorphism, Γ_g takes M_F, the F-isotropy subgroup of M, onto N_{gF}, the gF-isotropic subgroup of N. In turn, N_{gF} is conjugate under an inner automorphism of N to N_F. Thus M_F is conjugate to N_F under an inner automorphism of G_1. Since $M_F \subset N_F$, we have $\dim M_F = \dim N_F$, M_F is open and closed in N_F, and hence $M_F = N_F$. Thus, M_F is a maximal compact subgroup of G_F.

Now F being a covariant fibering, there is a transversal M' to F whose F-isotropic subgroup M'_F operate on F like a linear group and which permutes the fibers transitively. Since, by the foregoing, M'_F is a maximal

compact subgroup of the connected Lie group G_F, it is conjugate to M_F under an inner automorphism Γ_g with g in G_F. Since g keeps F invariant, M_F is equivalent to a linear group on $gf = F$. Moreover, M' being a maximal compact subgroup of the connected Lie group G_1, is conjugate to M by an inner automorphism of G_1. Hence M also permits the fibers transitively.

We now turn to a proof of the uniqueness of G-covariant fiberings of H up to equivalence in the sense that there exists a one-to-one bundle map between any two.

A covariant fibering $\mathfrak{F}$ is completely determined in view of Proposition 7.1 by the specification of a transversal M and a single fiber F. We shall employ the notation (M, F) for the covariant fibering $\mathfrak{F}$ which has M as transversal and F as fiber.

LEMMA 7.1. *Let (M, F) be a G-covariant fibering. Then (gMg^{-1}, gF) is a G-covariant fibering for any g in G and the map $x \to gx$ of H is a one-to-one bundle map of (M, F) onto (gMg^{-1}, gF).*

The verification of Lemma 7.1 is trivial.

LEMMA 7.2. *Let M be a transversal to the covariant fibering $\mathfrak{F}$, let p be a base point of M and let F be the fiber through p. Then $M_p = M_F$,* i.e., *$M \cap C_p$ is the subgroup of M which keeps F invariant.*

Proof. If we make use of the fact that M_F is equivalent to a linear group on F, then we infer that it keeps a point q fixed, i.e., $M_q = M_F$. Inasmuch as M_q is a maximal compact subgroup of C_q and C_q is conjugate to C_p under an inner automorphism, we find that M_p and M_q are conjugate under an inner automorphism since each is a maximal compact subgroup of conjugate connected Lie subgroups. M_p is a subgroup of the connected group M_F and, having the same dimension as M_F, must coincide with M_F.

LEMMA 7.3. *Let p be a base point of the transversal M. Then the orbit $M(p)$ has no tangent vector which is also tangent to a fiber.*

Proof. Let F_x denote the fiber through the point x, and let V_x denote the tangent space to F_x at x. Let U_x denote the tangent space to the orbit $M(p)$ at the point x in $M(p)$. It is clearly sufficient to prove that $U_p \cap V_p = (0)$. By the well known first fundamental theorem of Sophus Lie, the connected group M, considered as a transformation group operating (effectively) on H is generated by a linear family of infinitesimal transformations $\mathfrak{M}$ which can be identified with the Lie algebra of M. Let $\mathfrak{M}'$ denote the subalgebra of $\mathfrak{M}$ which generates the subgroup M_p. We denote by $\mathfrak{M}_x$

and $\mathfrak{M}'_x$ the element of contact which the distributions $\mathfrak{M}$ and $\mathfrak{M}'$ assign to the point x. Clearly, $\mathfrak{M}_p = U_p$ and $\mathfrak{M}'_p = (0)$.

Suppose now that $\mathfrak{M}_p \cap V_p \neq (0)$. Then there is an infinitesimal transformation X in $\mathfrak{M}$, but not in $\mathfrak{M}'$, such that X_p is in V_p. Now by definition of the exponential of an infinitesimal transformation, $X_{\exp X(q)}$ is the tangent vector to the parametrized path $\exp tX(p)$ at the point $t=1$; i.e., for any function f analytic on H around $\exp X(q)$, $(Xf)_{\exp X(q)} = df(\exp tX(q))/dt$ at $t=1$. Hence, X is tangent to the path $p(t)$ at all values of t, where $p(t)$ denotes the path $\exp tX(p)$.

On the other hand, $X_{p(t)}$ is the image of X_p under the differential of the transformation $\exp tX$, in view of the fact that $\exp tX$ carries the path $\exp sX$ (s varying) into the path $\exp(t+s)X(p)$. Since $\exp tX$ is a transformation in M, it permutes the fibers and hence its differential permutes the V_x with x in the orbit M. As a result, $X_{p(t)}$ is in $V_{p(t)}$ for all t and the path $\exp tX(p)$ is tangent to a fiber for each t.

Since a covariant fibering decomposes the differential structure of H, we may introduce a coordinate system $y_1, \cdots, y_n$ compatible with the differentiable structure of H such that in a neighborhood of p the fibers are slices $y_1 = \text{constant}, \cdots, y_f = \text{constant}$.

Since $p(t)$ is tangent to a fiber for each t, we have $dy_i(p(t))/dt = 0$ $(i = f, \cdots, n)$, and hence $y_i(p(t)) = \text{constant} = y_i(p(0))$. It follows immediately that $p(t)$ lies in the slice F_p. Since $\exp tX$ permutes fibers, it must be in M_F. By Lemma 7.2, $\exp tX$ is in M_p for each t and hence $X_p = 0$, contrary to hypothesis. Consequently, $U_p \cap V_p = (0)$.

LEMMA 7.4. *Let N be a compact group of transformations on a Euclidean space F which is equivalent to a linear group. Let p be any fixed point of N, let V be the tangent space to F at p. For each transformation g in N, let dg denote the differential of g at p. Then N is equivalent to the linear group dN acting on V with p corresponding to the zero vector and any element g of N corresponding to dg.*

Proof. By hypothesis, there is a coordinate system $x_1, \cdots, x_n$ on F (not necessarily differentiable) with respect to which M is a group of linear transformations. Since p is fixed under M, upon replacing each i-th coordinate function by $x_i - x_i(p)$, we arrive at a coordinate system in which M is a linear group and p is the origin. Thus without loss of generality we may assume that p is the origin of the coordinate system $x_1, \cdots, x_n$. By a result of Bochner (cf. [1]) there is a *neighborhood* $\mathcal{O}$ of the point p and differentiable mapping ϕ_1 of $\mathcal{O}$ onto a neighborhood of zero in V such that ϕ_1 is

equivariant with respect to the isomorphism d (that d is an isomorphism is well known; for expressing elements of the kernel N_d of d as linear parts plus terms of higher order, it is seen that no iterate of a transformation in N_d is of finite order and hence N_d, containing no non-unit elements of finite order, reduces to the unit).

We regard F as a linear space with $x_1, \cdots, x_n$ as a base of linear functions. Let $X_1, \cdots, X_n$ be a set of base vectors of F which lie in the neighborhood $\mathcal{O}$. By Bochner's result, $dg\phi_1(X_i) = \phi_1 g(X_i)$ $(i = 1, \cdots, n)$. We define the linear mapping ϕ of F onto V by the formula $\phi(\Sigma c_i X_i) = \Sigma c_i \phi(X_i)$. By linearity we get $dg\phi(X) = \phi g(X)$, all X in F_1. Hence, ϕ is equivariant with respect to d and N is equivalent to dN on V.

Note. ϕ may be non-differentiable with respect to the given differential structures of F.

LEMMA 7.5. *Let M be a transversal of a G-covariant fibering, F a fiber, p a point in F that is fixed under M_F, and C_p the isotropy subgroup of p. Then M_F operating on F is equivalent to* $\mathrm{Ad}\, M_F$ *on $\mathfrak{G}/\mathfrak{M} + \mathfrak{C}_p$ with p corresponding to zero, and m corresponding to the $\mathfrak{G}/\mathfrak{M} + \mathfrak{C}_p$ part of* $\mathrm{Ad}\, m$ *for m in M_p.*

Proof. Let H_p be the tangent space to H at p, let U_p be the tangent space to the orbit M_p at p and let V_p be the tangent space at p to the fiber F through p. Then H_p and U_p are the images of the Lie algebras $\mathfrak{G}$ and $\mathfrak{M}$ under the differential of the mapping $\pi: g \to g \cdot p$ of G onto the homogeneous space H. Now for any c in C_p and x in G, $\pi(cx) = \pi(cxc^{-1})$. Inasmuch as $c\pi(x) = \pi(cx)$ by definition of the operation of G on H, we have $c \cdot \pi = \pi \cdot \Gamma_c$, c in C_p. On taking the differential of this identity at the identity, we get $dc_p \cdot d\pi = d\pi \cdot \mathrm{Ad}\, c$, since $\mathrm{Ad}\, c$ is $d\Gamma_c$ at the identity. Denoting by dC_p the differentials of the transformations of H which are in C_p, we see that dC_p is equivalent to the operation of $\mathrm{Ad}\, C_p$ on $H_p = d\pi(G)$ which can be identified with $\mathfrak{G}/\mathfrak{C}_p$. In particular, the subgroup dM_p of differentials from M_p is equivalent to $\mathrm{Ad}\, M_p$ operating on $\mathfrak{G}/\mathfrak{C}_p$. By Lemma 7.3, V_p is complementary to U_p in H_p and hence dM_0, operating on V_p is equivalent to dM_p operating on H_p/U_p. Inasmuch as U_p corresponds to $\mathfrak{M} + \mathfrak{C}_p/\mathfrak{C}_p$ under the given identification of H_p with $\mathfrak{G}/\mathfrak{C}_p$, we conclude that dM_p ouerates on V_p as $\mathrm{Ad}\, M_p$ operates on $\mathfrak{G}/\mathfrak{C}_p/\mathfrak{M} + \mathfrak{C}_p/\mathfrak{C}_p = \mathfrak{G}/\mathfrak{M} + \mathfrak{C}_p$. Applying Lemma 7.4 and noting that $M_p = M_F$, by Lemma 7.2, we obtain the desired conclusion.

THEOREM 7. *Let G be a connected Lie group which operates transitively on the homogeneous space H with connected isotropy. Then any two G-*

covariant fiberings of H are equivalent decompositions, that is, there is a one-to-one bundle map of one onto the other.

Proof. By Lemma 7.1 we may restrict our attention to G-covariant fiberings with the same transversal M. Let therefore (M, F_1) and (M, F_2) be the two covariant fiberings. Inasmuch as the property of being a base point to M depends only on M, there is no generality lost in assuming that F_1 and F_2 contain the same base point p. By Lemma 7.2, $M_{F_1} = M_p = M_{F_2}$. By Lemma 7.5, there is a homeomorphism ϕ of F_1 onto F_2 such that $\phi(mf) = m\phi(f)$ for m in M_p and f in F_1. It follows immediately that the mapping $mf \to m\phi(f)$ for m in M, f in F_1, is a well defined homeomorphism which is a bundle map of (M, F_1) onto (M, F_2).

By an *isomorphism* of a fiber bundle we mean a one-to-one (bicontinuous) bundle map of it. Let M_i be a group of transformations on a bundle B_i $(i = 1, 2)$, and let ϕ be an isomorphism of B_1 onto B_2. We say ϕ send M_1 onto M_2 if $\phi M_1 \phi^{-1} = M_2$.

LEMMA 7.6. *Let M be a transversal to the G-covariant fiberings $\mathfrak{F}$. The base points of M are permuted transitively by the automorphism of $\mathfrak{F}$ which keep M invariant.*

Proof. Let p, p be any two base points to M and let F_1, F_2 be the fibers through them. Since (Prop. 7.1) M permutes the fibers transitively, we may assume without loss of generality that $F_1 = F_2 = F$. Hence, $M_{F_1} = M_{F_2} = M_F$.

If a linear space V and p_1, p_2 are fixed points of L, then the mapping $v \to v + (p_1 - p_2)$ of V is equivariant with respect to the identity automorphism. Since M_F is equivalent to a linear group on F, there is a homeomorphism ϕ of F onto itself such that $\phi(mf) = m\phi(f)$ for all m in M_F, f in F. As a result, $mf \to m\phi(f)$ with m in M and f in F is an automorphism of $\mathfrak{F}$ which carries p_1 into p_2. Since this automorphism keeps M invariant, the desired conclusion holds.

The above uniqueness result can be strengthened.

PROPOSITION 7.2. *Let F_i be a G-covariant fibering of H with transversal M_i and base point p_i $(i = 1, 2)$. Then there is an isomorphism of F_1 onto F_2 which carries p_1 onto p_2 and the transversal M_1 onto M_2.*

Proof. By Lemma 7.1, we reduce to the case that $M_1 = M_2$. Let F_1, F_2 denote the fibers of $\mathfrak{F}_1$, $\mathfrak{F}_2$ respectively that pass through p_1. From Lemma 7.5 it follows (just as in the proof of Theorem 7) that there is a mapping θ of F_1 onto F_2 such that the map $\phi_1 : mf \to m\theta(f)$ (m in M, f in F_1) is an isomorphism of $\mathfrak{F}_1$ onto $\mathfrak{F}_2$. Clearly, $\phi^{-1} m \phi = m$ for all m in M.

On the other hand, by Lemma 7.6, there is an automorphism ϕ_2 of $\mathfrak{F}_2$ which carries p_1 into p_2 and keeps M invariant. Hence $\phi_2\phi_1$ is an isomorphism of $\mathfrak{F}_1$ onto $\mathfrak{F}_2$ which sends p_1 onto p_2 and keeps M invariant. Proof of the proposition is now complete.

Remarks. In our uniqueness discussion for covariant fiberings, we made repeated use of the hypothesis that M_F is equivalent to a linear group on the fiber F. There is much ground for the suspicion that this hypothesis is superfluous in the sense that it is always true. That is, there is the well known conjecture of Samelson that any compact group of differentiable automorphisms of Euclidean space is equivalent to a linear group. In our case, even a weaker theorem is needed to conclude that M_F is equivalent to a linear group on F. Namely, let K be a compact subgroup of a Lie group G, and let F be a closed Euclidean (differentiable) subspace of a space H on which G acts transitively. If K keeps F invariant, it is equivalent to a linear group on F.

This conjecture appears to be difficult to prove even in the case that G is the group of rigid motions in Euclidean space and K is a subgroup of the orthogonal group.

THE JOHNS HOPKINS UNIVERSITY
AND
INSTITUTO DE MATEMATICA PURAE APLICADA, RIO DE JANEIRO.

REFERENCES.

[0] R. Arens, "Topologies for homeomorphism groups," *American Journal of Mathematics*, vol. 68 (1946), pp. 593-610.

[1] S. Bochner, "Compact groups of differentiable transformations," *Annals of Mathematics*, vol. 46 (1945), pp. 377-381.

[2] A. Borel and J. P. Serre, "Impossibilité de fibrer un espace Euclidien par des fibrés compactes," *Comptes Rendus de l'Académie des Sciences (Paris)*, vol. 230 (1950), pp. 2258-2260.

[3] E. Cartan, "Groupes simples clos et ouverts et géométrie Riemannienne," *Journal de Mathématiques Pures et Appliquées*, vol. 8 (1929), pp. 1-33.

[4] C. Chevalley, "On the topology of solvable groups," *Annals of Mathematics*, vol. 42 (1941), pp. 668-675.

[5] Feldbau, "Sur la classification des espaces fibrés," *Comptes Rendus de l'Académie des Sciences (Paris)*, vol. 208 (1939), pp. 1621-1623.

[6] K. Iwassawa, "On some types of topological groups," *Annals of Mathematics*, vol. 50 (1949), pp. 507-558.

[7] A. Malcev, "On the theory of Lie groups in the large," *Recueil Mathématique (Matematicheskii Sbornik)*, vol. 16 (58) (1945), pp. 163-189.

[8] D. Montgomery, "Simply connected homogeneous spaces," *Proceedings of the American Mathematical Society*, vol. 1 (1950), pp. 467-469.

[9] G. D. Mostow, "A new proof of E. Cartan's theorem on the topology of semi-simple groups," *Bulletin of the American Mathematical Society*, vol. 55 (1949), pp. 969-980.

[10] ———, "Some new decomposition theorems for semi-simple groups," *Memoirs of the American Mathematical Society*, (to appear).

[11] ———, "Factor spaces of solvable groups," *Annals of Mathematics*, vol. 60 (1954), pp. 1-27.

[12] A. Shapiro, "Cohomologie dans les espaces fibrés," *Comptes Rendus de l'Académie des Sciences (Paris)*, vol. 231 (1950), pp. 206-207.

[13] N. Steenrod, *The Topology of Fiber Bundles*, Princeton University Press, 1951.

[14] J. H. C. Whitehead, "On the decomposition of an infinitesimal group," *Proceedings of the Cambridge Philosophical Society*, vol. 32 (1936), pp. 229-237.

ON THE LIE AND JORDAN RINGS OF A SIMPLE ASSOCIATIVE RING.*

By I. N. HERSTEIN.

Given any associative ring A we can form, using its operations and its elements, two new rings. These use the elements of A and the addition as defined in A, but new multiplications are introduced to render them rings, albeit not necessarily associative rings. The first of these, the *Lie ring* A^L of A uses a multiplication defined by $[a, b] = ab - ba$ for any $a, b \in A$ where ab is the ordinary associative product of elements in A. The second of these, the *Jordan ring* of A, A^J, has its multiplication defined by $a \circ b = ab + ba$ for any pair of elements a, b in A.

Being defined in a manner so decidedly dependent on the associative product of A, it is natural to expect that an intimate relationship should exist between the structure of these two new rings and that of A. In this paper we study one phase of this relationship, namely the connection between the ideal structure of A as an associative ring with the ideal structure of A^L and A^J as Lie and Jordan rings respectively. To be more specific, we investigate how simplicity of A as an associative ring reflects into analogous properties of A^L and A^J.

When we say that U is an ideal of A^J, or, equivalently, when we say that U is a Jordan ideal of A, we mean that U is an additive subgroup of A and that for any $x \in U$ and any $y \in A$, $x \circ y = xy + yx$ is an element of U. We similarly define Lie ideals of A and ideals of A^L.

Although the main results of this paper deal with the case in which A is a simple ring, many of the other results do not require the assumption of simplicity in order to remain valid; so, unless otherwise stated, we make no assumption of simplicity for A.

1. The Jordan ring of A. We begin with

LEMMA 1. *If U is a Jordan ideal of A, and if a and b are elements of U, then for any x in A $(ab + ba)x - x(ab + ba)$ is an element of U.*

Proof. Since a is in U, a Jordan ideal of A, then for all $x \in A$, $a(xb - bx) + (xb - bx)a$ is also in U. But

* Received August 31, 1954.

$$a(xb-bx)+(xb-bx)a$$
$$=\{(ax-xa)b+b(ax-xa)\}+\{x(ab+ba)-(ab+ba)x\}$$

and since $b\in U$, the first term on the right hand side of this equation is in U; this, coupled with $a(xb-bx)+(xb-bx)a$ in U leads to $x(ab+ba)-(ab+ba)x\in U$, which is the lemma we set out to prove.

LEMMA 2. *If A is a simple ring of characteristic different from 2, and if U is a Jordan ideal of A, $U\neq A$, then any element a of U with the property that $ax-xa\in U$ for all x in A must necessarily satisfy $a=0$.*

Proof. By assumption, $ax-xa\in U$ for all $x\in A$. On the other hand, since U is a Jordan ideal of A, $ax+xa\in U$ for all x in A. Adding, we obtain that $2ax\in U$ for all $x\in A$. Since A is of characteristic $\neq 2$, $2A=A$, so we have that $ax\in U$ for all $x\in A$. However, for all y, since $ax\in U$, a Jordan ideal of A, $(ax)y+y(ax)\in U$; and since by the above $axy\in U$, we must have that $yax\in U$. In this way $AaA\subset U$. Since A is simple, $AaA=A$ unless $a=0$. Thus the lemma is established.

THEOREM 1. *If A is a simple ring of characteristic different from 2, then A^J is a simple Jordan ring.*

Proof. Suppose that $U\neq A$ is a Jordan ideal of A. For any $a,b\in U$ and any $x\in A$, by Lemma 1, $(ab+ba)x-x(ab+ba)$ is in U. Since $ab+ba$ is an element of U, by Lemma 2, $ab+ba=0$. In particular, $2a^2=0$, and so $a^2=0$ for any a in U. If $a\in U$, then for all $x\in A$, $ax+xa\in U$; so by the above, with $b=ax+xa$, we have that $a(ax+xa)+(ax+xa)a=0$; since $a^2=0$ we are left with $2axa=0$, and so, $axa=0$, for all $x\in A$. But then aA is a nilpotent right ideal of A, which is, of course, impossible in a simple ring unless $a=0$. Thus $U=(0)$ and we have proved that A^J is a simple Jordan ring.

(Note: the argument used in the proof of the above theorem actually can be refined to prove somewhat more, namely: if A is an associative ring such that no homomorphic image of A possesses nilpotent right ideals, then any Jordan ideal of A is at the same time an ordinary ideal of A. I owe this remark to Professor Irving Kaplansky.)

2. The Lie ring of A. For $a\in A$, by $[a,A]$ we shall mean the set $\{ax-xa \mid x\in A\}$. $[A,A]$ shall then represent the subgroup of A generated by all the commutators $xy-yx$ for all x, y in A. When we refer to an ideal of A we shall mean an ordinary, two-sided ideal of A under the associative multiplication of A.

A ring R, all of whose elements are nilpotent, is said to be *locally nilpotent* if the subring generated by any finite set of elements of R is

nilpotent. An ideal of R is said to be locally nilpotent if, as a ring, it is locally nilpotent.

We proceed to

THEOREM 2. *Let A be a ring with no non-zero locally nilpotent ideals. Suppose that in A, $2x=0$ implies that $x=0$. Suppose further that U, an associative subring of A, is also a Lie ideal of A. Then either U contains a non-zero ideal of A or U is contained in the center of A.*

Proof. Suppose first that U, as a subring of A, is not commutative. Then for some x, y in U, $xy-yx\neq 0$. Since U is a Lie ideal of A and since $x\in U$, $x(ys)-(ys)x$ is in U for every s in A. But $x(ys)-(ys)x=(xy-yx)s+y(xs-sx)$. Since $x\in U$ and since U is a Lie ideal of A, $xs-sx$ is in U; since U is, in addition, a subring of A and since y is also in U, $y(xs-sx)$ is in U. Thus from the above equation we have that $(xy-yx)s\in U$ for all $s\in A$. Thus for any $r\in A$, since U is a Lie ideal of A,

$$r(xy-yx)s-(xy-yx)sr=r\{(xy-yx)s\}-\{(xy-yx)s\}r\in U.$$

Knowing that $(xy-yx)sr\in U$ for all $r,s\in A$ from the argument above, we can now conclude that $r(xy-yx)s$ is in U for every r and s in A. In this way the ideal $A(xy-yx)A\subset U$. Hence if the theorem were false, $A(xy-yx)A=(0)$. This would force $(xy-yx)A$ to be a nilpotent ideal of A, which by assumption would mean that $(xy-yx)A=(0)$. $xy-yx$ would then become an absolute zero divisor, which is again impossible in a ring free from locally nilpotent ideals. So we have been forced into a contradiction. We must therefore suppose that U is a commutative subring of A.

We now propose to show that if U is a commutative ring then it must lie in the center of A. We assume that there is an $x\in U$ and an $s\in A$ so that $y=xs-sx\neq 0$. Since xs^2-s^2x is in U, a commutative ring, $x(xs^2-s^2x)=(xs^2-s^2x)x$. However, from $xs^2-s^2x=(xs-sx)s+s(xs-sx)$ we have that $x\{(xs-sx)s+s(xs-sx)\}=\{(xs-sx)s+s(xs-sx)\}x$. Since $xs-sx$ is also in U, it must commute with x; making use of this in the last equation above we obtain that $2(xs-sx)^2=0$. By assumption on A this leads to $(xs-sx)^2=0$. $y=xs-sx\neq 0\in U$, so for all $t\in A$, $(yt-ty)^2=0$. Since $y^2=0$, left multiplying $(yt-ty)^2=0$ by y and right multiplying it by t, we obtain that $(yt)^3=(0)$ for all $t\in A$. By a result of Levitzki [1] yA is a locally nilpotent right ideal. But then, by another result of Levitzki [2] AyA is a locally nilpotent ideal of A. In this way we arrive at a contradiction. So $y=0$, and x is in the center of A. That is, U is contained in the center of A.

It is generally well known, although to this author's knowledge nowhere in the literature, that a simple ring can not be locally nilpotent. For the

sake of completeness we record a proof of this here, since we must make use of it in the next theorem. So suppose that A is simple and locally nilpotent. Thus if $a \neq 0 \in A$, $AaA = A$. Thus for some $r_1, \cdots r_n, s_1, \cdots s_n$ in A

$$a = r_1 a s_1 + r_2 a s_2 + \cdots + r_n a s_n.$$

The subring T generated by $r_1, r_2, \cdots, r_n, s_1, \cdots, s_n$ is nilpotent, say $T^k = 0$. If we substitute the expression above for a in the right hand side for each a occurring we obtain $a = r_1' a s_1' + \cdots + r_t' a s_t'$, where the r_i' and s_i' are in T^2. Continuing this way we obtain such an expression for a where the multipliers on the right hand side come from T^{2^k}, and so are all 0; but then $a = 0$, a contradiction. This proves the assertion that a simple ring can not be locally nilpotent.

With this now established we have as an immediate corollary to Theorem 2

THEOREM 3. *If A is a simple ring of characteristic different from 2, then any proper Lie ideal of A which is at the same time a subring of A must lie in the center of A.*

LEMMA 3. *Let A be any associative ring, and let U be a Lie ideal of A. Let $T(U) = \{t \in A \mid [t, A] \subset U\}$. Then $T(U)$ is both a Lie ideal and a subring of A. Moreover $U \subset T(U)$.*

Proof. $T(U)$ is trivially a Lie ideal of A. Suppose that $a, b \in T(U), c \in A$. Then $(ab)c - c(ab) = \{a(bc) - (bc)a\} + \{b(ca) - (ca)b\}$, and since both a and b are in $T(U)$, the right hand side of this equation is in U. Thus $[ab, A] \subset U$, whence $ab \in T(U)$ and $T(U)$ is a subring of A. Since U is a Lie ideal of A, $U \subset T(U)$.

We are now in position to prove

THEOREM 4. *Let A be a simple ring of characteristic different from 2. Let U be a Lie ideal of A. Then either U is contained in the center of A or $U \supset [A, A]$.*

Proof. $T(U)$ is both a subring and a Lie ideal of A. By Theorem 3 either $T(U)$ is contained in the center of A or $T(U) = A$. If $T(U)$ is contained in the center of A, then so is U since $U \subset T(U)$. If, on the other hand $T(U) = A$, then by the very definition of $T(U)$, $[A, A] \subset U$.

3. Case of characteristic 2. Suppose that A is a simple ring of characteristic 2. Theorem 4 need no longer be true in this case. In fact, if A is the set of 2×2 matrices over a field Z of characteristic 2, or if A is a division algebra of dimension 4 over its center, a field of characteristic 2, then the theorem is definitely false. We propose to show that these constitute the only exceptions to our main result.

In the chain leading from Theorem 3 through Theorem 4, the characteristic of A does not enter. Thus we will consider those situations in which Theorem 3 fails to hold true in case A is of characteristic 2.

We suppose that A is a simple ring of characteristic 2. Suppose that U is both a Lie ideal and a subring of A and that $U \neq A$. From the Jacobi identity we obtain, as we did in the proof of Theorem 2, that if $x, y \in U$ and $s \in A$, then $(xy + yx)s \in U$. That is, $(xy + yx)A \subset U$. Hence as before, $A(xy + yx)A \subset U$. By the simplicity of A, $A(xy + yx)A$ is all of A unless $xy + yx = 0$; we are thus forced to assume that $xy + yx = 0$ for all x and y in U. If $U \subset Z$, the center of A, we have nothing left to prove. Suppose now that there exists an a in U and a is not in Z. Thus $as + sa \in U$ for all $s \in A$. Consequently $a(as + sa) + (as + sa)a = 0$ by the above; that is, $a^2 s = sa^2$ for all $s \in A$; so $a^2 \in Z$. Since $ar + ra \in U$, we also have that $(ar + ra)^2 \in Z$ for all $r \in A$. Should $Z = (0)$, then by the argument used in Theorem 2, Levitzki's theorems would apply, and would lead to a contradiction with the simplicity of A. So we can assume that $Z \neq (0)$. We can likewise assume that $a^2 \neq 0$ (for if $(ax + xa)^2 = 0$ for all x and if $a^2 = 0$, then Levitzki's theorems could again be used) for some $a \in U$, $a \notin Z$.

$Z \neq (0)$ is a field of characteristic 2. Since Z is not trivial, A is a primitive ring, and so is a dense ring of transformations on a vector space V over a division ring D. We want to first show that V is at most 2-dimensional over D, and from this to deduce that A is 4-dimensional over Z. If we extend Z to a field Z' we obtain a new simple ring A' and the dimension of A' over Z' is the same as the dimension of A over Z. Also, since $ax + xa$ and $ay + ya$ are in U for x, y in A, these two commutators always commute; from this it follows $(aw + wa)^2 \in Z'$ for all $w \in A'$. So all the properties of A carry over to A'. We make a special choice for Z', namely, since $a^2 = \lambda \in Z$, we define $Z' = Z(\sqrt{\lambda})$. Thus in A', $a^2 = \mu^2$, $\mu \in Z'$; the element $a' = a/\mu$ then satisfies $(a'w + wa')^2 \in Z'$ for all $w \in A'$ and $(a')^2 = 1$. All this discussion has achieved is that without loss of generality we may assume that in A there exists an element a, $a \notin Z$, $a^2 = 1$, $(ax + xa)^2 \in Z$ for all $x \in A$. On this basis we shall show that A is 4-dimensional over Z. Since $(a + 1)^2 = 0$, $a + 1 \neq 0$, A has zero divisors, so is not a division ring. As we noted earlier, A is a dense ring of linear transformations on a vector space V over a division ring D.

Let us first suppose that we can find v_1 and v_3 in V so that $v_1, v_2 = v_1 a$, $v_3, v_4 = v_3 a$ are linearly independent over D. Since A is dense on V there exists an $x \in A$ so that: $v_1 x = 0$, $v_2 x = 0$, $v_3 x = v_3$, $v_4 x = v_1$. Now $v_1(ax + xa) = v_2 x + 0 = 0$. Thus, since $(ax + xa)^2 \in Z$ and since $v_1(ax + xa)^2 = 0$, we must have that $(ax + xa)^2 = 0$. However, $v_3(ax + xa) = v_4 x + v_3 a = v_1 + v_4$,

so $0 = v_3(ax + xa)^2 = (v_1 + v_4)(ax + xa) = v_2 + v_3 \neq 0$ since v_2 and v_3 are linearly independent over D. Thus we arrived at a contradiction.

So we must assume that if $v_1, v_2 = v_1 a$, and v_3 are linearly independent over D then

$$v_3 a = v_1\lambda_1 + v_2\lambda_2 + v_3\lambda_3 \text{ with } \lambda_1, \lambda_2, \lambda_3 \in D. \tag{1}$$

Since D is the commuting ring of A and since $a^2 = 1$, this yields on right multiplication by a that

$$v_3 = v_3 a^2 = v_1\lambda_2 + v_2\lambda_1 + v_3 a\lambda_3. \tag{2}$$

From (1) and (2) it follows that $\lambda_1 = \lambda_2$, $\lambda_3 = 1$. Thus $v_3 a = (v_1 + v_2)\lambda + v_3$. From this we get that for all $v \in V$, $va = (v_1 + v_2)\lambda(v) + v$, where $\lambda(v) \in D$. There is a $y \in A$ so that $(ay + ya)^2 \neq 0$, for otherwise we could again use the Levitzki theorems (on $a + 1$) to reach a contradiction with the simplicity of A. But if $(ay + ya)^2 \neq 0 \in Z$, we may assume that $(ay + ya)^2 = 1$ (otherwise we would extend Z and proceed as we did with a in getting $a^2 = 1$). Now, $v(ya) = (v_1 + v_2)\lambda(vy) + vy$.

$$v(ay) = ((v_1 + v_2)\lambda(v) + v)y = (v_1 + v_2)\lambda(v)y + vy.$$

Adding $v(ya)$ and $v(ay)$ we obtain

$$v(ay + ya) = (v_1 + v_2)\lambda(vy) + (v_1 + v_2)\lambda(v)y.$$

Thus,

$$\begin{aligned} v &= v(ay + ya)^2 \\ &= (v_1 + v_2)(ay + ya)\lambda(vy) + (v_1 + v_2)y(ay + ya)\lambda(v). \end{aligned}$$

Letting $u_1 = (v_1 + v_2)(ay + ya)$ and $u_2 = (v_1 + v_2)y(ay + ya)$, we have shown that u_1 and u_2 constitute a basis of V over D. V is then 2 dimensional over D, contradicting that v_1, v_2 and v_3 were linearly independent over D.

So we have finally come down to this situation: given v, w in V, then v, va and w are linearly dependent over D. We claim that there is a v in V so that v and va are linearly independent over D. For if $va = v\lambda$, $\lambda \in D$, then $v = va^2 = v\lambda a = (va)\lambda = v\lambda^2$, so $\lambda^2 = 1$, hence $\lambda = 1$; and since $a \neq 1$, $v \neq va$ for some $v \in V$. Thus for this v, v and va are linearly independent over D. This, combined with the fact that v, va and w are linearly dependent for all $w \in V$, implies that w is a linear combination over D of v and va. Thus V is two dimensional over D. Since A is a dense ring of transformations on V over D, A must be all 2×2 matrices over D. All that remains now is to show that $D = Z$.

We have now reduced the whole problem to the following: let A be the set of all 2×2 matrices over a division ring D of characteristic 2; suppose that for some element $a \in A$, $a \notin Z$, a^2 is the unit matrix and $(ax + xa)^2$ is in

Z, the center, for all x in A; from this we want to conclude that $D = Z$, or what is equivalent in this case, namely that D is commutative.

Now, $a = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ where α, β, γ, δ, are in D. For any $r, s \in D$ we have that

$$\left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} r & s \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} r & s \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right\}^2 \in Z.$$

By carrying out the computations we see that the first element in the second row of this matrix $\{\ \}^2$ is the sum $\gamma r \alpha r + \gamma r^2 \alpha + \gamma r s \gamma + \gamma s \gamma r$. Hence this sum is 0 for all $r, s \in D$. In particular, if $s = 0$, $\gamma r \alpha r + \gamma r^2 \alpha = 0$. Thus the top identity reduces to $\gamma r s \gamma + \gamma s \gamma r = 0$ for all $r, s \in D$. If $\gamma \neq 0$, then $rs\gamma = s\gamma r$, and since $s\gamma$ runs through all the elements of D as s does, we have $rt = tr$ for all $r, t \in D$, whence D is commutative. So we suppose that $\gamma = 0$. Using the element $\begin{pmatrix} r & 0 \\ s & 0 \end{pmatrix}$ of A and proceeding as before, we obtain that $\beta = 0$. It follows that a^2 is the unit matrix. From this we have $\alpha^2 = \delta^2 = 1$; since we are in a division ring of characteristic 2, this means that $\alpha = \delta = 1$, and so a is the unit matrix forcing it to lie in Z, contrary to supposition. In this way we have proved that D is commutative.

Thus A has now become revealed as nothing but a total matrix algebra of degree 2 over a commutative field of characteristic 2. In the course of the proof we have extended the center Z on several occasions, possibly changing A somewhat, but under these various extensions *the dimensions of the new rings over their centers have not changed.* Thus we have shown that Theorem 3 is correct even in characteristic 2, provided A is not 4-dimensional over its center. This then leads us to our principal theorem:

THEOREM 5. *If A is a simple ring and if U is a Lie ideal of A, then either U is contained in the center of A, or else U contains $[A, A]$, except in the case that A is a 4-dimensional simple algebra over its center, which is a field of characteristic 2.*

THE UNIVERSITY OF PENNSYLVANIA.

REFERENCES.

[1] J. Levitzki, "A problem of A. Kurosh," *Bulletin of the American Mathematical Society*, vol. 52 (1946), pp. 1033-1035.

[2] ———, "On the radical of a general ring," *ibid.*, vol. 49 (1943), pp. 462-466.

SOLUTION OF SOME PROBLEMS OF DIVISION.*[1]

Part II. Division by a Punctual Distribution.

By LEON EHRENPREIS.

In Part I of this series [3] it was shown that every constant-coefficient partial differential equation possesses an elementary solution and, moreover, if D is any polynomial of derivation and S a distribution of finite order, then the equation

$$D * T = S \tag{1}$$

has a solution T which is a distribution of finite order. Moreover, if S is an indefinitely differentiable function, we can choose for T an indefinitely differentiable function. In this paper, we shall extend the above results to the case in which D is any punctual distribution (that is, linear combination of derivatives of measures which represent masses concentrated at a single point). Thus, the results for differential equations are extended to differential-difference equations with constant coefficents. In particular, every differential-difference equation with constant coefficients has an elementary solution.

The idea of the proof is to use the space $\boldsymbol{D}_F$ (see [3]) which, with a slightly different topology, is the Fourier transform of the space $\mathcal{D}$ of L. Schwartz (see [7]). Under Fourier transformation, the distribution D goes over into an exponential polynomial P. We then must show that, if $PF_\alpha \to 0$ in $\boldsymbol{D}_F$, then also $F_\alpha \to 0$ in $\boldsymbol{D}_F$. This results from a certain minimum modulus property of P which we shall explain now in case we are dealing with distributions on the real line. Then P is an exponential polynomial of one variable, and has a certain "periodic" nature (see [6]): There exists an $L > 0$ so that, in every interval of the real axis of length L, there is a point at which the modulus of P does not get too small. Also, P is an entire function of exponential type. Thus, by using the minimum modulus results of [5], we can produce certain circles on which the modulus of P does not get too small. Once this is established, the result follows as in [3] for pure polynomials by means of the maximum modulus principle.

All the results of this paper can be extended to systems of equations as in [3].

* Received August 31, 1954.

[1] Work partially supported by National Science Foundation grant NSF 5-G1010.

The notation of this paper will be that of Part I of this series (see [3], Section 2), and the results of that paper will be used here in an essential way.

2. Solution of the problem. By an exponential polynomial we shall mean here a linear combination of products of polynomials by pure imaginary exponentials. Given any punctual distribution E, there is an exponential polynomial $Q = \boldsymbol{F}E$ such that, for any $f \in \mathcal{D}$, $\mathcal{F}(E * f) = QF$ (see [4], [7]); conversely, any exponential polynomial Q may be written as $\boldsymbol{F}E$ for some punctual distribution E.

Let Q be an exponential polynomial different from zero one one variable, and write $Q = Q_1 \exp(ia_1 \cdot) + \cdots + Q_k \exp(ia_k \cdot)$, where the Q_j are polynomials $\not\equiv 0$ and where $a_1 < a_2 < \cdots < a_k$. Call $L = a_k - a_1$ and let $Q_1 = b_0 X^m + b_1 X^{m-1} + \cdots + b_m$. (It is allowed that $b_0 = 0$.)

LEMMA 1. *In the above notation, there exists a $K > 0$ which depends only on $a_1, a_2, \cdots, a_k$ and on the degrees of Q_j such that each interval I in the complex plane which is parallel to the real axis and has length $\geqq 2(L+1)$ contains a point y at which*

$$|Q(y)| \geqq K |b_0| \exp(-|a_1 \alpha|), \tag{2}$$

where α is the distance of I from the real axis.

Remark. In case $L = 0$, this is an easy consequence of the results of [3].

Proof. Let c be the midpoint of I, and call $S = \tau_{-c} Q$. Then S is again an exponential polynomial. Moreover, the exponentials that occur in S are the same as those that occur in Q and, for each exponential, the polynomial coefficient is of the same degree in S as in Q. In addition, if b_0' denotes the coefficient of $X^m \exp(ia_1 \cdot)$ in S, then

$$|b_0'| \geqq |b_0| \exp(-|a_1 \alpha|). \tag{3}$$

Now, let us use the theory of mean-periodic functions of L. Schwartz (see [6]). We can find a measure u whose carrier is contained in $[-L-1 \leqq x \leqq L+1]$ which depends only on $a_1, a_2, \cdots, a_k$ and the degrees of the polynomial coefficients of $\exp(ia_j \cdot)$ such that $b_0' = \int S du$. Let v be some point in $|x| \leqq L+1$ at which S attains its maximum. Then, if K^{-1} denotes the total variation of u,

$$|b_0'| = \left|\int S du\right| \leqq K^{-1} |S(v)| \text{ or } |S(v)| \geqq K |b_0'| \geqq K |b_0| \exp(-|a_1 \alpha|),$$

by (3). The result follows immediately.

LEMMA 2. *With Q as above, suppose that $|(\tau_x Q)(z)| \leqq M(x)\exp(l|z|)$ for all complex numbers x, z, where M is a positive function and $l > 0$. Let y be any complex number which satisfies (2). Then for any $r > 0$ we can describe a circle about y of radius r' such that $r \leqq r' \leqq 2r$ and*

$$\min_{|z|=r'} |Q(z)| \geqq M(y)^B \exp(clr') K^d |b_0|^d \exp(-d|a_1\alpha|),$$

where B, c, and d are constants and where d is a positive integer.

Proof. This is just Theorem 5 of Section 4 of [5].

Now, let D be a punctual distribution different from zero and let $P = \boldsymbol{F}D$. By $P\boldsymbol{D}_F$ we denote the space of functions PG for $G \in \boldsymbol{D}_F$ with the topology induced by $\boldsymbol{D}_F$ (see [3]). The space $D * \mathcal{D}_F$ is defined similarly.

THEOREM 1. *$PG \to G$ is a continuous linear map of $P\boldsymbol{D}_F \to \boldsymbol{D}_F$.*

Proof. The proof will be by induction on the number of letters p which occur in P. For $p = 0$, P is a non-zero constant and the result is obvious. Let $p > 0$ and assume that the theorem is proven for all exponential polynomials in fewer than p letters. Without loss in generality, we may assume that we can write

$$P(z) = [P_0(z_2, \cdots, z_p)z_1^m + P_1(z_2, \cdots, z_p)z_1^{m-1} + \cdots + P_m(z_2, \cdots, z_p)]$$
$$\times \exp(ia_1 z_1) + Q_2(z_1, \cdots, z_p)\exp(ia_2 z_1) + \cdots + Q_k(z_1, \cdots, z_p)\exp(ia_k z_1),$$

where the P_j and the Q_j are exponential polynomials (the exponentials occurring in the Q_j being independent of z_1) with $P_0 \not\equiv 0$, and where $a_1 < a_2 < \cdots < a_k$. The proof will be completed if we can show that $PF \to P_0{}^d F$ is a continuous linear map of $P\boldsymbol{D}_F \to P_0{}^d \boldsymbol{D}_F$, where d is the constant that appears in Lemma 2.

This map being obviously linear, we need prove continuity only at zero. Let N be a neighborhood of zero in $P_0{}^d \boldsymbol{D}_F$. By Theorem 7 of [3] we can find a finite sequence of polynomials $A_1, \cdots, A_t$ and an increasing sequence of positive numbers b_l, so that N contains the set of $G \in P_0{}^d \boldsymbol{D}_F$ which satisfy, for all l,

$$\max_{z \in C^j \cap C_{b_l}} |\exp(ilp_j \cdot z) A_r(z) G(z)| \leqq 1,$$

for $r = 1, 2, \cdots, t$ and $j = 1, 2, \cdots, 2^n$.

For any complex number x, let $x^* \in C$ be the point $(x, 0, \cdots, 0)$. Then it is easily verified that $\tau_{x^*} P = \boldsymbol{F}[\exp(ix^* \cdot)D]$, where $\exp(ix^* \cdot)D$ is the punctual distribution defined by $\exp(ix^* \cdot)D \cdot g = D \cdot \exp(ix^* \cdot)g$ (see [4], [7]). From this it follows immediately that we can find positive numbers a, b, β such that, for any complex number x and any $z \in C$,

$$(4) \qquad |(\tau_{x^*} P)(z)| \leqq a(1 + |x|)^\beta \exp(\gamma(|z_1| + \cdots + |z_n|)).$$

Set $L = a_k - a_1$ and let q be an integer $> d\,|\,a_1\,|$. For each l, set $c_l = b_{l+q} + 4(L+1)$. Let s, T be positive constants to be specified later, and let $A_1', A_2', \cdots, A_{st}'$ be the polynomials $TA_1, \cdots, TA_t$, $TXA_1, \cdots, TXA_t$, $\cdots, TX^sA_1, \cdots, TX^sA_t$.[2] Let N' be the set of $G \in P\boldsymbol{D}_F$ which satisfy, for each l, v, j,

$$\max_{z \in C^j \cap C_{c_l}} |\exp(ilp_j \cdot z) A'_v(z) G(z)| \leqq 1,$$

so that N' is a neighborhood of zero in $P\boldsymbol{D}_F$. We claim that, for a proper choice of T and s, $PG \in N'$ implies $P_0{}^d G \in N$.

Let $G \in \boldsymbol{D}_F$ be so chosen that $PG \in N'$; fix j and l and let $(z_1, \cdots, z_n) \in C^j \cap C_{b_l}$. We assume that $I(z_1) \geqq 0$, the other case being treated similarly. Denote by P' the exponential polynomial in one variable: $z' \to P(z', z_2, \cdots, z_p)$, and $P_0' = P_0(z_2, \cdots, z_p)$. Let I be the interval in the complex plane which is parallel to the real axis, center z_1, length $2(L+1)$. By Lemma 1 we can find a point $z_0 \in I$ such that $|P'(z_0)| \geqq K\,|\exp(i\,|\,a_1\,|\,z_0)|\,|P_0'|$, where K is independent of $(z_1, z_2, \cdots, z_n)$. By Lemma 2 and the above, we can describe about z_0 a circle of radius r' with $2(L+1) \leqq r' \leqq 4(L+1)$ such that, for all z' on this circle,

$$|P'(z')| \geqq \delta(1 + |z'|)^B |P_0'|^d |\exp(id\,|\,a_1\,|\,z_0)|, \tag{5}$$

where B, d, and δ are independent of $(z_1, z_2, \cdots, z_n)$.

Now, for any z' on the circle $|z - z_0| = r'$, $(z, z_2, \cdots, z_n)$ lies in $C_{c_{l-q}}$ if $l \geqq q$, or in C_{c_0} if $l < q$. Moreover by (5), for any z' on this circle and any v,

$$\begin{aligned} |P_0'|^d |A_v(z', z_2, \cdots, z_n) G(z', z_2, \cdots, z_n) \exp(ilp_j \cdot (z', z_2, \cdots, z_n))| \\ \leqq \eta\,|\exp(-id\,|\,a_1\,|\,z_0 + iqz) \exp(i(l-q)p_j \cdot (z', z_2, \cdots, z_n))\,| \\ \times |A_v(z', z_2, \cdots, z_n) P(z', z_2, \cdots, z_n)(1 + |z'|)^{-B} G(z', z_2, \cdots, z_n)|, \end{aligned} \tag{6}$$

where η is a constant independent of $(z_1, z_2, \cdots, z_n)$. Now,

$$|\exp(-id\,|\,a_1\,|\,z_0 + iqz')| \leqq \exp 4(L+1)q,$$

because $q \geqq d\,|\,a_1\,|$. It follows easily from this that we can choose s and T independent of $(z_1, z_2, \cdots, z_n)$ and of G, l, j, so that the right side of (6) is $\leqq 1$. By the maximum modulus theorem, we also have

$$|P_0'|^d |A_v(z_1, z_2, \cdots, z_n) G(z_1, z_2, \cdots, z_n) \exp(ilp_j \cdot (z_1, z_2, \cdots, z_n))| \leqq 1.$$

We have proven that $PG \to P_0{}^d G$ is a continuous linear map of $P\boldsymbol{D}_F \to P_0{}^d \boldsymbol{D}_F$. But, $P_0{}^d$ is an exponential polynomial in fewer than p

[2] X is the polynomial $X(z_1, \cdots, z_n) = z_1$.

variables. Thus, by our induction hypothesis, $PG \to G$ is a continuous linear map of $P\boldsymbol{D}_F \to \boldsymbol{D}_F$, which is the desired result.

From the above we have

COROLLARY. *$g \to D * g$ is a topological isomorphism of $\mathcal{D}_F$ onto $D * \mathcal{D}_F$.*

THEOREM 2. *For any $S \in \mathcal{D}_F'$ there exists a $T \in \mathcal{D}_F'$ such that $D * T = S$. In particular, every differential-difference equation with constant coefficients possesses an elementary solution in $\mathcal{D}_F'$.*

Proof. It is easily seen that $\check{D}$ is a punctual distribution (see [4]).[3] Now, $\check{D} * g \to S \cdot g$ is a continuous linear function T on $\check{D} * \mathcal{D}_F$, because it is the composition of the continuous linear maps $\check{D} * g \to g$ and $g \to S \cdot g$. By the Hahn-Banach theorem (see [1]), T can be extended to a continuous linear function on $\mathcal{D}_F$, that is, to an element $T \in \mathcal{D}_F'$. We have, for any $g \in \mathcal{D}_F$ (see [4]),

$$D * T \cdot g = T \cdot \check{D} * g = T \cdot \check{D} * g = S \cdot g.$$

Thus, $D * T = S$, which is the desired result.

The case $S = \delta$ (Dirac's measure) shows that D has an elementary solution (see [7]).

For any $l > 0$, $P\boldsymbol{D}_l$ is the space of PG for $G \in \boldsymbol{D}_l$ with the topology induced by $\boldsymbol{D}$; the spaces $D * \mathcal{D}_l$ are defined similarly. $D * \mathcal{E}'$ is the space of $D * S$ for $S \in \mathcal{E}'$ with the topology induced by $\mathcal{E}'$; $D * \mathcal{E}$ is defined similarly.

THEOREM 3. *For any $l > 0$, $PG \to G$ is a continuous linear map of $P\boldsymbol{D}_l \to \boldsymbol{D}_l$.*

Proof. It is clear that, for some $m > 0$, $P\boldsymbol{D}_l \subset \boldsymbol{D}_m$. The result now follows from Theorem 1 and the fact that the spaces $P\boldsymbol{D}_j$, $\boldsymbol{D}_j$ have the topologies induced by $\boldsymbol{D}_F$ (see [3]).

COROLLARY. *For any $l > 0$, $g \to D * g$ is a topological isomorphism of $\mathcal{D}_l$ onto $D * \mathcal{D}_l$.*

THEOREM 4. *$S \to D * S$ is a topological isomorphism of $\mathcal{E}'$ onto $D * \mathcal{E}'$.*

Proof. The map is one-to-one by the Paley-Wiener theorem (see [4], [7]) and is clearly continuous, linear, and onto. We must therefore verify continuity, at zero, of the inverse. By the results of [4], the topology of $\mathcal{E}'$ can

[3] For any $S \in \mathcal{D}'$, $\check{S}$ is the distribution $\check{S} \cdot f = \overline{S \cdot \check{f}}$ for any $f \in \mathcal{D}$. Our definition of convolution differs slightly from that of Schwartz (see [4]).

be described as follows: A fundamental system of neighborhoods of zero in $\mathcal{E}'$ consists of those sets N for which we can find a compact set $K \subset \mathcal{D}_F$ and a neighborhood of zero M in $\mathcal{D}_F$ so that N consists of those $S \in \mathcal{E}'$ for which $S * f \in M$ for all $f \in K$.

Let N be a neighborhood of zero in $\mathcal{E}'$, so we can find a compact set $K \subset \mathcal{D}_F$ and a neighborhood of zero M in $\mathcal{D}_F$, so that N contains the set of $S \in \mathcal{E}'$ which satisfy $S * f \in M$ for all $f \in K$. By the corollary to Theorem 1, $D * M$ is a neighborhood of zero in $D * \mathcal{D}_F$. Let U be the set of all $D * \check{T} \in \mathcal{E}'$ for which $(D * \check{T}) * g \in D * M$ for all $g \in K$, so U is a neighborhood of zero in $D * \mathcal{E}'$. We claim that $D * \check{T} \in U$ implies $T \in N$. For, if $D * \check{T} \in U$ and $g \in K$ (see [4]), $D * (T * g) = (D * \check{T}) * g \in D * M$. Thus, $T * g \in M$, which means that $T \in N$. This completes the proof of Theorem 4.

THEOREM 5. *$f \to D * f$ is a continuous linear map of $\mathcal{E}$ onto $\mathcal{E}$.*

Proof. The continuity and linearity of the map are clear. Let $g \in \mathcal{D}$; then $h : \check{D} * S \to S \cdot g$ is a continuous linear function $\check{D} * \mathcal{E}'$, since it is the composition of the continuous linear maps: $\check{D} * S \to S$ and $S \to S \cdot g$. h can be extended to a continuous linear function h on $\mathcal{E}'$ by the Hahn-Banach theorem. Now, $\mathcal{E}$ is reflexive (see [7]), so there exists a $k \in \mathcal{E}$ with $h \cdot T = T \cdot k$ for all $T \in \mathcal{E}'$. Thus, for any $S \in \mathcal{E}'$ (see [4]),

$$S \cdot D * k = \check{D} * S \cdot k = h \cdot \check{D} * S = h \cdot \check{D} * S = S \cdot g.$$

By the Hahn-Banach theorem, $D * k = g$, which is the desired result.

3. General remarks. The method developed in Section 2 can be used to solve other types of division problems. Let us consider first the case where $n = 1$. Let S be a distribution whose Fourier transform (see [4]) can be repersented as $\mathfrak{e}(F)$ where F is an entire function of finite order which is slowly increasing on the real axis.[4] Now (see [4] or [5]), $f \to S * f$ does *not* map $\mathcal{D}_F \to \mathcal{D}_F$ unless S is of compact carrier. But, suppose that F is mean-periodic. Then, for certain spaces $\mathfrak{D}$ of functions whose Fourier transforms are spaces of entire functions, $f \to S * f$ maps $\mathfrak{D} \to \mathfrak{D}$ and the analog of the corollary to Theorem 1 can be proven for these spaces by means of the formal development (see [6]) of mean-periodic functions, and by use of the methods of Section 2.

In case $n > 1$, we need additional hypotheses (besides mean-periodicity of F) in order to guarantee that our induction procedure will work. This

[4] For G a slowly increasing function, $\mathfrak{e}(G)$ is the element of $\boldsymbol{D}'$:

$$e(G) \cdot H = \int G(x) H(x)\, dx \qquad \text{for any } H \in \boldsymbol{D}.$$

is because no analog of the formal development of L. Schwartz is known for $n > 1$. It is, however, not difficult to see what hypotheses on S will be sufficient to make our induction procedure work.

The above method will be discussed at length in a future publication.

THE JOHNS HOPKINS UNIVERSITY AND THE INSTITUTE FOR ADVANCED STUDY.

REFERENCES.

[1] S. Banach, *Théorie des Opérations Linéaires*, Warsaw, 1932.

[2] J. Dieudonné and L. Schwartz, "La dualité dans les espaces ($\mathcal{F}$) et ($\mathcal{LF}$)," *Annales de l'Institut Fourier (Grenoble)*, vol. 1 (1950), pp. 61-101.

[3] L. Ehrenpreis, "Solutions of some problems of division, Part I. Division by a polynomial of derivation," *American Journal of Mathematics*, vol. 76 (1954), pp. 883-903.

[4] ———, "Analytic functions and the Fourier transform of distributions," to appear in the *Annals of Mathematics*.

[5] ———, "Mean periodic functions, Part I. Varieties whose annihilator ideals are principal," *American Journal of Mathematics*, vol. 77 (1955), pp. 293-328

[6] L. Schwartz, "Théorie générale des fonctions Moyenne-periodique," *Annals of Mathematics*, vol. 48 (1947), pp. 857-929.

[7] ———, *Theorie des Distributions*, vol. I-II, Paris, 1950-1951.

MEAN PERIODIC FUNCTIONS.*[1]

Part I. Varieties Whose Annihilator Ideals are Principal.

By LEON EHRENPREIS.

1. Introduction. Let C be complex Euclidean n-space. By $\mathcal{H}$ we denote the space of entire functions in n complex variables with the topology of uniform convergence on the compact sets of C; thus, $\mathcal{H}$ is a complete, reflexive, locally convex, metrizable, topological vector space. We shall say that $f \in H$ is *mean-periodic* (see [12]) if the linear combinations of its translates are not dense in $\mathcal{H}$. Denote by $\mathcal{H}'$ the dual of $\mathcal{H}$ with the topology of uniform convergence on the bounded sets of $\mathcal{H}$. (Since the closed bounded sets of $\mathcal{H}$ are compact, $\mathcal{H}'$ is also given the topology of uniform convergence on the compact sets of $\mathcal{H}$.) Then $f \in \mathcal{H}$ is mean periodic if and only if there exists an $S \in \mathcal{H}'$ such that the convolution $S * f = 0$ (see Proposition 5 of Section 2). Let f be mean periodic; our two fundamental problems are the following: Let V be the closure of the set of linear combinations of translates of f. *Does V contain an exponential polynomial?* (An exponential polynomial is a linear combination of products of exponentials by monomials.) If the answer to the former question is in the affirmative, then *is every $g \in V$ the limit of the exponential polynomials of V?*

More generally, let W be any non-empty set in $\mathcal{H}$ with W different from $\{0\}$ which is closed with respect to translations, linear combinations, and the topology of $\mathcal{H}$. We shall call such a set a *variety*. An example of such is the set V above. Now, we can ask the same two questions for W as were asked for V above. In case $n = 1$, these two questions were answered in the affirmative by L. Schwartz (see [12]) and, moreover, it was shown by him that every variety is the closure of the set of linear combinations of the translates of some $f \in \mathcal{H}$. The present paper is consecrated towards giving a partial extension of these results to the case $n > 1$.

Let W be a variety. Denote by W' the set of all $S \in \mathcal{H}'$ for which $S * f = 0$ for every $f \in W$. It is easily seen that this is the same as the set of $S \in \mathcal{H}'$ such that $S(f) = 0$ for every $f \in W$. It is clear that W' is a closed ideal (under convolution) in $\mathcal{H}'$. W' is called the *annihilator ideal* of W.

* Received August 31, 1954; revised January 14, 1955.

[1] Work supported by National Science Foundation Grants NSF5-G205 and NSF5-G1010.

The main result of this paper is the following: Let W be a variety whose annihilator ideal is principal. Then W contains an exponential polynomial and, moreover, each $f \in W$ is the limit of exponential polynomials of W. Thus, any two varieties with the same exponential polynomials are identical, i.e., a variety is completely determined by its exponential polynomials. Another way of putting this is: Let V be the variety generated by the exponential polynomials of W, that is, V is the closure, in H, of the exponential polynomials of W; then $V = W$.

Naturally, the question arises as to whether the above result can be extended to other spaces instead of $\mathcal{H}$. It will be seen that the possibility of extension depends on the ideal theory of the Fourier transform of the space in question. In fact, our main problem is the following: Let $\mathcal{K}$ be a topological ring consisting of entire functions. When is every closed principal ideal in $\mathcal{K}$ determined by its local ideals (see [3])? We shall show that the answer is in the affirmative if $\mathcal{K}$ is

1. The ring $\mathcal{H}$ of entire functions (this was shown in [3]).
2. The ring of entire functions of exponential type.
3. The ring of polynomials.
4. The ring of entire functions of finite order.

Naturally, it is possible to extend the above to other rings.

We shall also present here a simplified version of the solution to the fundamental problems of mean periodic functions in case that $n = 1$ even for varieties whose annihilator ideals are non-principal. (The first solution was given by L. Schwartz in [12].)

In part II of this series we shall consider nonprincipal annihilator ideals and arbitrary n.

The principal results of this paper were obtained in the Spring of 1953 while the author was under contract NSF S-G205 with the National Science Foundation. I have learned from Professor L. Schwartz that Malgrange has since obtained similar results and has extended them to other spaces of distributions of Schwartz (see [10]).

Unless otherwise specified, all cross references in this paper refer to the section in which they are given. If, for example, in Section 3 we refer to Proposition 1, it will be understood that the reference is to Proposition 1 of Section 3.

2. Fourier transform and convolution in $\mathcal{H}'$. For any $x \in C$, x_j is the j-th component of x; by $\| x \|$ we mean $| x_1 | + | x_2 | + \cdots + | x_n |$. and we

define $|x| = \max(|x_1|, |x_2|, \cdots, (x_n|)$. If $x, y \in C$, then $x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n$, and $\exp(x\cdot)$ is the function on $C: y \to \exp(x \cdot y)$. If f is an entire function of n complex variables, we shall say that f is of exponential type $\leqq a$ (where $a \geqq 0$) if, for any $\epsilon > 0$,

$$f(x) = O[\exp(a + \epsilon)\|x\|)].$$

The exponential type of f is the g. l. b. of all a which satisfy the above relation. For any $S \in \mathfrak{H}'$, $f \in \mathfrak{H}$, we shall usually write $S \cdot f$ instead of $S(f)$ with a similar notation for other dual spaces.

Let $S \in \mathfrak{H}'$; since the topology of $\mathfrak{H}$ is that induced by the space J of continuous functions on C with the topology of uniform convergence on the compact sets of C, S can be extended to a continuous linear function u on J. Now u is, by definition, a measure of compact carrier on C, so that we may write, for $f \in \mathfrak{H}$, $S \cdot f = \int f\, du$. By the *Fourier transform* of S we mean the function M on C:

$$M(z) = S \cdot \exp(iz\cdot) = \int \exp(iz \cdot t)\, du(t) = (\boldsymbol{F}(S))(z).$$

It follows immediately from the fact that u is of compact carrier that the integral above converges uniformly for z in any compact set of C, so that M is an entire function. A simple argument shows that M is an entire function of exponential type. Since the set $\{\exp(-iz\cdot)\}_{z \in C}$ is dense in $\mathfrak{H}$, it follows that M determines S uniquely. (Of course, there are infinitely many measures which represent S, any two of which differ by a measure which is zero on $\mathfrak{H}$.)

Conversely, let N be a given entire function of exponential type on C. Then we wish to show that N is the Fourier transform of some $S \in \mathfrak{H}'$. In case $n = 1$, this follows from a theorem of Borel (see [12], also [16], p. 286). In case of $n > 1$, the result can be proven in a similar manner, but we shall give a different proof because it is also applicable to other situations. Before giving the proof, we shall need a few preliminary considerations.

Denote by $\boldsymbol{H}'$ the space of Fourier transforms of elements of $\mathfrak{H}'$ with the topology to make $\boldsymbol{F}: \mathfrak{H}' \to \boldsymbol{H}'$ a topological isomorphism. For c any complex number, $\mathfrak{I}(c)$ is the imaginary part of c, $\mathfrak{R}(c)$ is the real part of c. For any $b > 0$, C_b is the set of $z = (z_1, z_2, \cdots, z_n) \in C$ such that, for each j, $|\mathfrak{I}(z_j)| \leqq b$. For $j = 1, 2, \cdots, n$, we denote by Z_j the function on $C: z \to z_j$. For any $S \in \mathfrak{H}'$, and any integers $k_1, k_2, \cdots, k_n$,

$$S_{k_1k_2\ldots k_n} = S \cdot Z_1^{k_1} Z_2^{k_2} \cdots Z_n^{k_n}.$$

Now, if $f \in \mathfrak{H}$, let $f(z) = \sum f_{k_1k_2\ldots k_n} z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n}$ be the Taylor expansion

of f at zero. Then it is clear that the series $\sum f_{k_1k_2\dots k_n}Z_1^{k_1}Z_2^{k_2}\cdots Z_n^{k_n}$ converges to f in $\mathcal{H}$. Thus,

$$S\cdot f=\sum S_{k_1k_2\dots k_n}f_{k_1k_2\dots k_n}, \tag{1}$$

the series being known to be convergent. The particular choice of $f=\exp(iz\cdot)$ yields

$$S\cdot\exp(iz\cdot)=(\boldsymbol{F}(S))(z) \tag{2}$$
$$=\sum(i^{k_1+k_2+\cdots+k_n}/k_1!k_2!\cdots k_n!)S_{k_1k_2\dots k_n}Z_1^{k_1}Z_2^{k_2}\cdots Z_n^{k_n}.$$

We have proven

PROPOSITION 1. *For any $S\in\mathcal{H}'$, $(i^{k_1+k_2+\cdots+k_n}/k_1!k_2!\cdots k_n!)S_{k_1k_2\dots k_n}$ are the coefficients in the Taylor expansion of $\boldsymbol{F}(S)$ at zero. In particular, $(i^{k_1+k_2+\cdots+k_n}/k_1!k_2!\cdots k_n!)S_{k_1k_2\dots k_n}$ are the Taylor coefficients, at zero, of an entire function of exponential type.*

It is not very difficult to show directly that the numbers $S_{k_1k_2\dots k_n}$ render the right side of equation (1) convergent whenever $f_{k_1k_2\dots k_n}$ are the Taylor coefficients of an entire function, if and only if $(i^{k_1k_2\cdots k_n}/k_1!k_2!\cdots k_n!)S_{k_1k_2\dots k_n}$ are the Taylor coefficients of an entire function of exponential type. (This will be discussed in great detail in a forthcoming article by the author on infinite derivatives.) From this it is not difficult to show that every entire function of exponential type is the Fourier transform of some $S\in\mathcal{H}'$. However, we prefer to give still a third proof, since it will help to illuminate the structure of the topology of $\boldsymbol{H}'$.

The following proposition describes the convergence of sequences in $\boldsymbol{H}'$. By a similar method we could describe the bounded sets of $\boldsymbol{H}'$. Since $\mathcal{H}'$ is known to be bornologic (that is, a subset N of $\mathcal{H}'$ is a neighborhood of zero if, for any bounded set B in $\mathcal{H}'$, we can find a $b>0$ so that $bB\subset N$), we have a complete description of the topology of $\boldsymbol{H}'$.

PROPOSITION 2. *Let $\{f^j\}$ be a sequence of entire functions of exponential type which are in $\boldsymbol{H}'$. A necessary and sufficient condition that $f^j\to 0$ in $\boldsymbol{H}'$ is that there exist an $a>0$ such that*

$$\max_{x\in C}|e^{-a\|x\|}f^j(x)|\to 0. \tag{3}$$

Denote by S^j the inverse Fourier transform of f^j. Then, if (3) is satisfied, we even have $S^j\cdot h\to 0$ uniformly on the set of h which satisfy

$$\max_{|x|\leqq a}|h(x)|\leqq 1. \tag{4}$$

Proof. Suppose first that $f^j \to 0$ in $\boldsymbol{H}'$. It is known [2] that this implies that $S^j \cdot k \to 0$ uniformly for k in some neighborhood of zero. Thus, there exists an $a > 0$ so that $S^j \cdot k \to 0$ uniformly on the set N of k which satisfy $\max_{|x| \leqq a} |k(x)| \leqq 1$. For any $z \in C$, we clearly have $e^{-a\|z\|} \exp(iz\cdot) \in N$ from which (3) follows immediately.

For any h satisfying (4), denote by $h_{k_1 k_2 \ldots k_n}$ the Taylor coefficients of h at zero. Then we may write (see [2])

$$h_{k_1 k_2 \ldots k_n} = (1/(2\pi i)^n \int_\Gamma (h(z)/z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n})\, dz$$

where we may take for the chain Γ the cartesian product of the n circles, center origin, radius a, which lie in each of the coordinate plans. Thus,

$$|h_{k_1 k_2 \ldots k_n}| \leqq a^{-(k_1+k_2+\cdots+k_n)}. \tag{5}$$

From (3) it follows easily that, if $f^j{}_{k_1 k_2 \ldots k_n}$ denote the Taylor coefficients of f^j, then, given $\epsilon > 0$, we can find a J so large that, for $j > J$ and all $k_1, k_2, \cdots, k_n$,

$$f^j{}_{k_1 k_2 \ldots k_n} \leqq \epsilon a^{k_1+k_2+\cdots+k_n}/k_1!k_2! \cdots k_n!.$$

Thus, by Proposition 1, for any h satisfying (3),

$$\begin{aligned} |S^j \cdot h| &= |\sum f^j{}_{k_1 k_2 \ldots k_n} h_{k_1 k_2 \ldots k_n}| \\ &\leqq \epsilon \sum 1/k_1!k_2! \cdots k_n! = \epsilon e^n. \end{aligned}$$

This means that $S^j \cdot h \to 0$ uniformly for all h satisfying (4); since this set of h is clearly a neighborhood of zero in $\mathcal{H}$, we have the desired result.

From Proposition 2 we deduce immediately

PROPOSITION 3. *Let $\{f^j\}$ be a sequence in $\boldsymbol{H}'$ and a, b and $\delta < a$ be positive numbers such that, for all j,*

$$|f^j(x)| \leqq b \exp[(a - \delta)\|x\|] \text{ for any } x \in C. \tag{6}$$

Suppose moreover that $f^j \to 0$ in the topology of $\mathcal{H}$. Then also $f^j \to 0$ in the topology of $\boldsymbol{H}'$. Moreover, if S^j denotes the inverse Fourier transform of f^j, then $S^j \cdot h \to 0$ uniformly for all h which satisfy (4).

PROPOSITION 4. *The topology of $\boldsymbol{H}'$ is stronger than that induced by $\mathcal{H}$.*

Proof. Let B be a filter base in $\mathcal{H}'$ which converges to 0; let K be a compact set in C. For any $f \in \mathcal{H}$, denote by $B \cdot f$ the filter base obtained from B by replacing each S of B by $S \cdot f$. Now, it is clear that $\{\exp(iz\cdot)\}_{z \in K}$

[2] See, for example, [14], vol. I, p. 91, where a similar result is proven for the space $\mathcal{E}$ of Schwartz.

is a bounded set in H. Thus, the filter bases $B \cdot \exp(iz\cdot)$ for $z \in K$ converge uniformly to zero. The result follows from the definition of the Fourier transform.

THEOREM. *$\boldsymbol{H}'$ consists of all entire functions of exponential type. An entire function f is of exponential type $\leqq c$ if and only if, for any $\epsilon > 0$, the inverse Fourier transform S of f can be represented by a measure u whose carrier is contained in $C^{c+\epsilon}$.*

(For any $d > 0$, C^d is the set of all $z \in C$ such that $|z| \leqq d$.)

Proof. The sufficiency of the condition being easily verified, we pass to the necessity. Denote by K the vector space of all entire functions of exponential type, so that $\boldsymbol{H}' \subset K$; we want to show that $\boldsymbol{H}' = K$. Now, we know that every polynomial is in $\boldsymbol{H}'$; we shall show that, for any $f \in K$, we can find a sequence of polynomials f^j which converge to f in the topology of $\mathfrak{H}$ and such that $\{f^j\}$ is a Cauchy sequence in $\boldsymbol{H}'$. Since the space $\boldsymbol{H}'$ is known to be complete, we shall deduce that $f \in \boldsymbol{H}'$.

To this end, let $f_{k_1 k_2 \ldots k_n}$ be the Taylor coefficients of f at the origin. Define

$$f^j = \sum_{k_1+k_2+\ldots+k_n \leqq j} f_{k_1 k_2 \ldots k_n} Z_1^{k_1} Z_2^{k_2} \cdot \cdot \cdot Z_n^{k_n}.$$

Then it is clear that $f^j \to f$ in the topology of $\mathfrak{H}$. Moreover, it follows from Proposition 3 that $\{f^j\}$ is a Cauchy sequence in $\boldsymbol{H}'$. Since $\boldsymbol{H}'$ is complete, we can find a $g \in \boldsymbol{H}'$ such that $g = \lim f^j$, the limit being taken in $\boldsymbol{H}'$. Now, by Proposition 4, $g = \lim_{\mathfrak{K}} f^j$, from which it follows that $g = f$.

It follows also from Proposition 3 that, for any $\epsilon > 0$, S is bounded on the set of $h \in \mathfrak{H}$ which satisfy

$$\max_{|x| \leqq c+\epsilon} |h(x)| \leqq 1.$$

Thus, S can be represented by a measure of carrier contained in $C^{c+\epsilon}$ which is the desired result.

For any $f \in \mathfrak{H}$, $z \in C$, we denote by $\tau_z f$ the function on C: $(\tau_z f)(x) = f(x - z)$; it is clear that $\tau_z f \in \mathfrak{H}$. $\tau_z f$ is called the *translate* of f by z. We see easily that $(z, f) \to \tau_z f$ is a continuous map of $C \times \mathfrak{H}$ into $\mathfrak{H}$ and also that, for $f \in \mathfrak{H}$, $z \to \tau_z f$ is an analytic map of C into $\mathfrak{H}$ over every region in the complex plane (see [8]).

Now, for any $f \in \mathfrak{H}$, $S \in \mathfrak{H}'$, we define the convolution $S * f$ by $(S * f)(z) = S \cdot \tau_{-z} f$ for any $z \in C$. If u is any measure which represents S, then we have

$$(S * f)(z) = \int f(x + z)\, du(x).$$

From the integral expression above, it is clear that $S * f \in \mathfrak{H}$.

PROPOSITION 5. *For any $S \in \mathcal{H}'$, $f \in \mathcal{H}$, $S * f$ is the limit in $\mathcal{H}$ of linear combinations of translates of f.*

Proof. Let u be a measure of compact carrier representing S and let K be a compact set in C. Then, by the continuity of translation, $\{\tau_{-z}f\}_{z \in K}$ is a bounded set in $\mathcal{H}$; this set of functions is thus equicontinuous on every compact set of C, hence on a compact set $U \subset C$ whose interior contains the carrier of u. It follows from the theory of the Riemann-Stieltjes integral that, given any $\epsilon > 0$, we can find points $x_1, x_2, \cdots, x_r$ in U and complex numbers $u_1, u_2, \cdots, u_r$ such that, for all $z \in K$,

$$\left| \int \tau_{-z}f \, du - \sum u_j (\tau_{-z}f)(x_j) \right| \leqq \epsilon$$

or, what is the same thing,

$$\left| (S * f)(z) - \sum u_j (\tau_{-x_j}f)(z) \right| \leqq \epsilon,$$

from which the result follows.

PROPOSITION 6. *If B is any bounded set in $\mathcal{H}$, then $S \to S * f$ are, for $f \in B$, equicontinuous linear maps of $\mathcal{H}' \to \mathcal{H}$. If K is any bounded set in $\mathcal{H}'$, then $f \to S * f$ are, for $S \in K$, equicontinuous linear maps of $\mathcal{H} \to \mathcal{H}$.*

Proof. Since the maps are both clearly linear, we need verify equicontinuity only at zero. Let N be a neighborhood of zero in H; we can find positive numbers a, b such that N contains the set of $f \in H$ for which $\max_{|x| \leqq a} |f(x)| \leqq b$. By the continuity of translation, the set $\{\tau_{-z}f\}_{|z| \leqq a, f \in B} = B'$ is bounded in $\mathcal{H}$. Let M be the neighborhood of zero in $\mathcal{H}'$ consisting of all $S \in \mathcal{H}'$, such that $|S \cdot g| \leqq b$ for all $g \in B'$. Then clearly, for $S \in M$, $f \in B$, we have $S * f \in N$.

On the other hand, since H is metrizable, hence bornologic (see [6]), we can find a neighborhood of zero P in H such that $|S \cdot f| \leqq b$ for all $S \in K$, $f \in P$. Let Q be a neighborhood of zero in $\mathcal{H}$ such that, for all $f \in Q$, $|z| \leqq a$, we have $\tau_{-z}f \in P$. Then, for $S \in K$, $f \in Q$ we clearly have $S * f \in N$.

For any S, $T \in \mathcal{H}'$, the convolution $S * T \in \mathcal{H}'$ is defined by $S * T \cdot f = S \cdot T * f$ for any $f \in \mathcal{H}$. ($S * T$ is in $\mathcal{H}'$ by Proposition 6.)

PROPOSITION 7. *$S, T \to S * T$ is a continuous bilinear map of $\mathcal{H}' \times \mathcal{H}' \to \mathcal{H}'$. Moreover, $S * T = T * S$.*

Proof. The map being obviously bilinear, we need verify continuity only at zero. Let N be a neighborhood of zero in $\mathcal{H}'$ and B a bounded set in $\mathcal{H}'$. Then, there is a bounded set $K \subset \mathcal{H}$ so that N contains the set of all

$S \in \mathcal{H}'$, such that $|S*f| \leqq 1$ for all $f \in K$. By Proposition 5, the set $U = \{T*f\}_{T \in B, f \in K}$ is bounded in $\mathcal{H}$. Thus, there is a neighborhood M of zero in $\mathcal{H}'$ such that, for $S \in M$, $g \in U$, $|S \cdot g| \leqq 1$. Hence, for $S \in M$, $T \in B$, $S*T \in N$.

Now, let u be a measure of compact carrier representing S, and v a measure of compact carrier representing T. Then, for any $f \in H$,

$$S*T \cdot f = S \cdot T*f = \int du(z) \int f(x+z)\, dv(x)$$
$$= \int dv(x) \int f(x+z)\, du(z) = T \cdot S*f = T*S \cdot f.$$

Thus, $T*S = S*T$.

From the above it follows that, if V is any bounded set in $\mathcal{H}'$, then $T \to S*T$ are, for $S \in V$, equicontinuous maps of $\mathcal{H}' \to \mathcal{H}'$. Thus, in the terminology of J. Dieudonné and L. Schwartz (see [6], [7]), $S, T \to S*T$ is a separately continuous bilinear map of $\mathcal{H}' \times \mathcal{H}' \to \mathcal{H}$. Since H is a complete metrizable space (hence of type $(\mathcal{F})$), this map must be continuous.

Now, let us describe $S*f$ in terms of the Taylor coefficients of f and $\boldsymbol{F}(S)$ at zero. Let u be a measure of compact carrier which represents S. Then we see easily that, if t denotes the map of $C \to H : t(x) = \tau_{-x} f$, then $\int t\, du$ defines the function $S*f$ of $\mathcal{H}$. It follows that, if D is any operator of partial differeniation of the form $D = \partial^{k_1+k_2+\cdots+k_n}/\partial Z_1^{k_1} \partial Z_2^{k_2} \cdots \partial Z_n^{k_n}$, then we have

$$(D(S*f))(0) = \int (Df)\, du. \tag{7}$$

We have thus

PROPOSITION 8. *For any integers $k_1, k_2, \cdots, k_n$, and any $S \in \mathcal{H}'$, $f \in \mathcal{H}$, we have*

$$(S*f)_{k_1 k_2 \ldots k_n} = \sum S_{l_1 l_2 \ldots l_n} f_{l_1+k_1, l_2+k_2, \ldots, l_n k_n}, \tag{8}$$

the sum on the right being extended over all integers $l_1, l_2, \cdots, l_n$, the series on the right being absolutely convergent.

From this we deduce

THEOREM 2. *For any $S, T \in \mathcal{H}'$,*

$$\boldsymbol{F}(S*T) = \boldsymbol{F}(S)\boldsymbol{F}(T). \tag{9}$$

Proof. From (8) we have, for any $f \in \mathcal{H}$,

$$S*T \cdot f = S \cdot T*f = \sum S_{k_1 k_2 \ldots k_n} (T*f)_{k_1 k_2 \ldots k_n} \tag{10}$$
$$= \sum_{k_1 k_2, \cdots, k_n} S_{k_1 k_2 \ldots k_n} \sum_{l_1 l_2, \cdots, l_n} T_{l_1 l_2 \ldots l_n} f_{l_1+k_1, l_2+k_2, \ldots, l_n+k_n}.$$

Now, $S_{k_1k_2\cdots k_n}/k_1!k_2!\cdots k_n!$ and $T_{l_1l_2\cdots l_n}/l_1!l_2!\cdots l_n$ are the Tayor coefficients, at the origin, of entire functions of exponential type. Thus, we can find an $a>1$ so that

$$S_{k_1k_2\cdots k_n}=O(a^{k_1+k_2+\cdots+k_n}), \text{ and } T_{l_1l_2\cdots l_n}=O(a^{l_1l_2+\cdots+l_n}).$$

Since f is an entire function,

$$f_{k_1k_2\cdots k_n}=O((na)^{-(k_1+k_2+\cdots+k_n)}).$$

Using these estimates we have, for some $\alpha>0$,

$$\begin{aligned}&|f_{k_1+l_1,+k_2+l_2,\ldots,k_n+l_n}S_{k_1k_2\cdots k_n}T_{l_1l_2\cdots l_n}|\\ &\leqq\sum\alpha(na)^{-(k_1+k_2+\cdots+k_n)-(l_1+l_2+\cdots+l_n)}a^{k_1+k_2+\cdots+k_n}a^{l_1+l_2+\cdots+l_n}\\ &=\alpha\sum n^{-(k_1+k_2+\cdots+k_n)-(l_1+l_2+\cdots+l_n)}.\end{aligned}$$

Since the number of lattice points in real $2n$ dimensional Euclidean space in the circle of center origin, radius r is $O(r^{2n})$, the series above clearly converges. Thus, we may interchange the order of summation in (10) to obtain

$$\begin{aligned}S*T\cdot f&=\sum_{k_1k_2\cdots k_n}S_{k_1k_2\cdots k_n}\sum_{l_1l_2\cdots l_n}T_{l_1-k_1,\,l_2-k_2,\ldots,\,l_n-k_n}f_{l_1l_2\cdots l_n}\\ &=\sum_{l_1l_2\cdots l_n}f_{l_1l_2\cdots l_n}\sum_{k_1k_2\cdots k_n}S_{k_1k_2\cdots k_n}T_{l_1-k_1,\,l_2-k_2,\ldots,\,l_n-k_n}.\end{aligned}$$

We conclude that the coefficients of the Taylor expansion of $\boldsymbol{F}(S*T)$ at the origin are

$$\begin{aligned}\boldsymbol{F}(S*T)_{l_1l_2\cdots l_n}&=S_{k_1k_2\cdots k_n}T_{l_1-k_1,\,l_2-k_2,\ldots,\,l_n-k_n}\\ &=\boldsymbol{F}(S)\boldsymbol{F}(T)_{l_1l_2\cdots l_n}.\end{aligned}$$

Thus, $\boldsymbol{F}(S*T)=\boldsymbol{F}(S)\boldsymbol{F}(T)$, which is the desired result.

Remark. Theorem 2 could be easily proven by direct use of the definitions, but we have preferred the above proof because it illustrates the relationship between the Fourier transform and the Taylor coefficients of entire functions. This relationship will be made the object of a detailed study by the author in a forthcoming paper on infinite derivatives.

From this we have immediately

COROLLARY. *For* $S,\ T,\ U\in\mathcal{H}'$, $S*(T*U)=(S*T)*U$, *that is, convolution is associative.*

Let us denote by $\boldsymbol{H}$ the dual of $\boldsymbol{H}'$, since $\mathcal{H}$ is a reflexive, $\mathcal{H}$ is top-

ologically isomorphic to $\boldsymbol{H}$, the topological isomorphism which we denote by $\boldsymbol{F}$ being given by

$$\boldsymbol{F}(f)\cdot\boldsymbol{F}(S)=S\cdot f,$$

for any $f\in\mathcal{H}$, $S\in\mathcal{H}'$. For any $a\in C$ and any non-negative integers $k_1,k_2,\cdots,k_n$, we denote by $\delta_a^{k_1k_2\cdots k_n}$ the element of $\boldsymbol{H}$

$$\delta_a^{k_1+k_2+\cdots+k_n}f=i^{k_1+k_2+\cdots+k_n}[(\partial^{k_1+k_2+\cdots+k_n}/\partial Z_1^{k_1}\partial Z_2^{k_2}\cdots\partial Z_n^{k_n})f](a), \tag{11}$$

for any $f\in\mathcal{H}'$.

PROPOSITION 9. *For any $a\in C$ and any integers $k_1,k_2,\cdots,k_n$, we have*

$$\boldsymbol{F}(Z_1^{k_1}Z_2^{k_2}\cdots Z_n^{k_n}\exp(ia\cdot))=\delta_a^{k_1k_2\cdots k_n}. \tag{12}$$

Proof. For any $S\in\mathcal{H}'$, write $f=\boldsymbol{F}(S)$; then

$$\begin{aligned}S\cdot Z_1^{k_1}Z_2^{k_2}\cdots Z_n^{k_n}\exp(ia\cdot)&=S\cdot\sum[(ia)^{l_1+l_2+\cdots+l_n}/l_1!l_2!\cdots l_n!]Z_1^{k_1+l_1}Z_2^{k_2+l_2}\cdots Z_n^{k_n+l_n}\\&=\sum[(ia)^{l_1+l_2+\cdots+l_n}/l_1!l_2!\cdots l_n!]S_{k_1+l_1,k_2+l_2,\ldots,k_n+l_n}\\&=\delta_a^{k_1k_2\cdots k_n}\cdot f,\end{aligned}$$

by Taylor's formula (see [2]), where for $a=(a_1,a_2,\cdots,a_n)$ we have written $(ia)^{l_1+l_2+\cdots+l_n}$ for $i^{l_1+\cdots+l_n}a_1^{l_1}a_2^{l_2}\cdots a_n^{l_n}$.

We shall sometimes consider the formula (11) for $f\in\mathcal{H}$ as defining the element $\delta_a^{k_1k_2\cdots k_n}\in\mathcal{H}'$.

3. The spectrum of a variety. By the results of Section 2, we may consider $\mathcal{H}$ as a topological module, under convolution, over the commutative topological ring $\mathcal{H}'$. By Proposition 5 of Section 2 and the fact that, for $f\in\mathcal{H}$, $a\in C$, $\delta_a*f=\tau_{-a}f$, we see that the varieties of $\mathcal{H}$ are exactly the closed submodules of $\mathcal{H}$ which are stable under $\mathcal{H}'$. Moreover, by Proposition 6 of Section 2, the annihilator ideal of any variety is closed.

By an *ideal* in $\mathcal{H}'$ ($\boldsymbol{H}'$) we shall mean a closed ideal different from $\mathcal{H}'$ ($\boldsymbol{H}'$). Let I be an ideal in $\mathcal{H}'$ and consider the set W of $f\in\mathcal{H}$ for which $S\cdot f=0$ for all $S\in I$. We claim that W is a variety. By the Hahn-Banach theorem, W is not reduced to $\{0\}$. Let $f\in W$; we claim that, for any $T\in\mathcal{H}'$, $T*f$ is again in W. For, if $S\in I$, then

$$S\cdot T*f=S*T\cdot f=0,$$

because $S*T\in I$. Thus, W is stable under $\mathcal{H}'$; since W is closed by Proposition 6 of Section 2, W is a variety. We call W the *annihilator variety* of I.

PROPOSITION 1. *Let W be a variety and W' its annihilator ideal. Then the annihilator variety of W' is W. Conversely, if I is an ideal and I' its annihilator variety, then I is the annihilator ideal of I'.*

This is an immediate result of a general theorem on bipolars in topological vector spaces (see [6]).

Proposition 1 shows us that the correspondence between varieties and their annihilator ideals is a one-one correspondence between the varieties of $\mathcal{H}$ and the ideals of $\mathcal{H}'$. Under Fourier transform, this yields a one-one correspondence between the varieties of $\mathcal{H}$ and the ideals in the ring $\boldsymbol{H}'$ of entire functions of exponential type. Thus, any problem involving the varieties of H can be translated into a problem in the theory of ideals in rings of analytic functions.

Our main task now is to translate the fundamental problems of mean periodic functions into problems about the ring $\boldsymbol{H}'$. Let us note the following first: Let W be a variety and $Z_1^{k_1}Z_2^{k_2}\cdots Z_n^{k_n}\exp(a\cdot)\in W$. Then, since derivation is the limit of linear combinations of translations, it follows that $Z_1^{l_1}Z_2^{l_2}\cdots Z_n^{l_n}\exp(a\cdot)\in W$ whenever $l_1\leqq k_1, l_2\leqq k_2,\cdots, l_n\leqq k_n$. Now, let us denote by $\{a_j\}$ a fixed ordering of the 2^n-1 sequences $j_1, j_2,\cdots, j_r$ for $1\leqq j_1<j_2<\cdots<j_r\leqq n$ and any $r\leqq n$. Then, for any $j=1,2,\cdots,2^n-1$, let $a_j=j_1, j_2,\cdots, j_r$ and let $z\in C$; we call s_j the j-th *part of the spectrum of W at z*, where s_j is the set of r-tuples $(l_1, l_2,\cdots, l_r)$, such that

$$Z_{j_1}^{l_1}Z_{j_2}^{l_2}\cdots Z_{j_r}^{l_r}\exp(z\cdot)\in W$$

but, for no r-tuple $(k_1, k_2,\cdots, k_r)$ with $k_1\geqq l_1, k_2\geqq l_2,\cdots, k_r\geqq l_r$ and some $k_p>l_p$, is $Z_{j_1}^{k_1}Z_{j_2}^{k_2}\cdots Z_{j_r}^{k_r}\exp(z\cdot)\in W$. In some cases, we may have to allow some of the l_p in some of the r-tuples of s_j to be infinity, for example, the r-tuple $(\infty, \infty, l_3, l_4,\cdots, l_r)$ will be part of s_j if

$$Z_{j_1}^{l_1}Z_{j_2}^{l_2}\cdots Z_{j_r}^{l_r}\exp(z\cdot)\in W$$

for any integers l_1, l_2, but no $r-2$ tuples $(k_3, k_4,\cdots, k_r)$ with

$$k_3\geqq l_3, k_4\geqq l_4,\cdots, k_r\geqq l_r$$

which is different from $(l_3, l_4,\cdots, l_r)$ can be used in place of $l_3, l_4,\cdots, l_r$. By the *spectrum of W* we mean the set of 2^n-tuples $(a, s_1, s_2,\cdots, s_{2^n-1})$ where $\exp(a\cdot)\in W$ and s_j is the j-th part of the spectrum of W at a.

Thus defined, the spectrum of W is indeed a very complicated affair, since each s_j consists of a finite, but unbounded, number of r-tuples of integers. In case that $n=1$, it is clear that s_1 (which is the only s_j that appears) is

just a single integer. Thus, in this case, our spectrum coincides with the spectrum as defined by L. Schwartz [12].

Now, let I be an ideal in $\boldsymbol{H}'$. By the *cospectrum of* I we mean the spectrum of the annihilator variety of the inverse Fourier transform of I. By Proposition 9 of Section 2, we may describe the cospectrum of I as follows: The cospectrum of I consists of all 2^n tuples $(a, s_1, s_2, \cdots, s_{2^n-1})$ such that a is a common zero of all the functions of I and, for each j, if a_j corresponds to the sequence $j_1, j_2, \cdots, j_r$ then s_j is the set of r-tuples $(l_1, l_2, \cdots, l_r)$ such that, for any $f \in I$,

$$[(\partial^{l_1+l_2+\cdots+l_r}/\partial Z_{j_1}{}^{l_1}\partial Z_{j_2}{}^{l_2}\cdots\partial Z_{j_r}{}^{l_r})f](a) = 0, \tag{1}$$

but for no other r-tuple $(k_1, k_2, \cdots, k_r)$ with $k_1 \geqq l_1, k_2 \geqq l_2, \cdots, k_r \geqq l_r$ is equation (1) satisfied for all $f \in I$. In some cases, we may have to allow some of the l_p to be infinity; the definition in that case is analogous to the definition of the spectrum when infinity appeared in some of the r-tuples.

From our previous remarks it follows that if $(l_1, l_2, \cdots, l_r)$ is such that equation (1) is satisfied for all $f \in I$, then if $k_1 \leqq l_1, k_2 \leqq l_2, \cdots, k_r \leqq l_r$, equation (1) is satisfied for all $f \in I$ with $(k_1, k_2, \cdots, k_r)$ replacing $(l_1, l_2, \cdots, l_r)$.

For any two varieties V, W, we shall say that the spectrum of V is contained in the spectrum of W if every exponential polynomial of V is in W. For two ideals I, J in $\boldsymbol{H}'$, we say that the cospectrum of I is contained in the cospectrum of J if the spectrum of the annihilator variety of the inverse Fourier transform of I is contained in the spectrum of the annihilator variety of $\boldsymbol{F}^{-1}(J)$. This is the same as saying:

If $(z, s_1, s_2, \cdots, s_{2^n-1})$ is in the cospectrum of I, then for any j, if $a_j = j_1, j_2, \cdots, j_r$ and if $(l_1, l_2, \cdots, l_r)$ is an r-tuple of s_j, then equation (1) holds for all $f \in J$. (With a suitable modification if some $l_p = \infty$.)

For any $f \in \boldsymbol{H}'$ and any ideal I of $\boldsymbol{H}'$, we denote by fI the closure of the set of fg for $g \in I$, so fI is again an ideal. We shall show later that, in fact, $\{fg\}_{g \in I}$ is itself closed. If J is another ideal in $\boldsymbol{H}'$, we write IJ for the closure of $\{fg\}_{f \in I,\, g \in J}$.

Now, let V, W be two varieties. Then clearly, $V \cap W$ is again a variety, or $\{0\}$. By $V + W$ we denote the smallest variety containing V and W (this is easily seen to be the closure of the set of $f + g$ for $f \in V, g \in W$). We have the obvious

PROPOSITION 2. *Let V, W be varieties, and V', W' their respective annihilator ideals. Then the annihilator ideal of $V + W$ is $V' \cap W'$, and the annihilator ideal of $V \cap W$ is $V' + W'$ (the smallest ideal containing V' and W') or $\mathfrak{A}'$ if $V \cap W = \{0\}$.*

We shall now introduce three operations on the spectra (or cospectra). Let V and W be varieties and M, P their respective spectra.

(a) The *spectral intersection* $M \cap P$ consists of all 2^n-tuples $(z, s_1, s_2, \cdots, s_{2^n-1})$ such that there exist 2^n-tuples $(z, m_1, m_2, \cdots, m_{2^n-1}) \in M$ and $(z, p_1, p_2, \cdots, p_{2^n-1}) \in P$, with the property that if $(l_1, l_2, \cdots, l_r)$ is an r-tuple of s_j, then there exist r-tuples $(k_1, k_2, \cdots, k_r)$ of m_j and $(q_1, q_2, \cdots, q_r)$ of p_j such that $l_1 \leqq k_1, l_2 \leqq k_2, \cdots, l_r \leqq k_r, l_1 \leqq q_1, l_2 \leqq q_2, \cdots, l_r \leqq q_r$. In addition, if $(l_1, l_2, \cdots, l_r)$ is in s_j, then there is no other r-stuple $(t_1, t_2, \cdots {}_1 t_r)$ in s_j with $t_1 \leqq l_1, t_2 \leqq l_2, \cdots, t_r \leqq l_r$. (Of course, suitable modifications have to be made with infinity.)

(b) The *spectral sum* $M + P$ consists of all 2^n-tuples $(z, s_1, s_2, \cdots, s_{2^n-1})$ such that there exists either a 2^n-tuple $(z, m_1, m_2, \cdots, m_{2^n-1}) \in M$ or a 2^n-tuple $(z, p_1, p_2, \cdots, p_{2^n-1})$ with the properties that

1. If there is no 2^n-tuple $(z, m_1, m_2, \cdots, m_{2^n-1}) \in M$, then $s_j = p_j$ for all j.

2. If there exists no 2^n-tuple $(z, p_1, p_2, \cdots, p_{2^n-1}) \in P$, then $s_j = m_j$ for all j.

3. If both 2^n-tuples exist, then for each j we form s_j' as the collection of all r-tuples that belong to both p_j and m_j. In this case s_j is the largest subset of s_j' that fulfills the condition that, if $(l_1, l_2, \cdots, l_r)$ is in s_j and if $(k_1, k_2, \cdots, k_r)$ is another r-tuple with $k_1 \leqq l_1, k_2 \leqq l_2, \cdots, k_r \leqq l_r$, then $(k_1, k_2, \cdots, k_r) \in s_j$.

(c) The *spectral product* MP consists of those 2^n-tuples $(z, s_1, s_2, \cdots, s_{2^n-1})$ for which there exists a 2^n-tuple

$$(z, m_1, m_2, \cdots, m_{2^n-1}) \in M \text{ or } (z, p_1, p_2, \cdots, p_{2^n-1}) \in P$$

such that

1. If $(z, m_1, m_2, \cdots, m_{2^n-1})$ does not exist, then $s_j = p_j$ for all j.

2. If $(z, p_1, p_2, \cdots, p_{2^n-1})$ does not exist, then $s_j = m_j$ for all j.

3. If both exist then, for each j we form the set s_j' consisting of all r-tuples of the form $(k_1 + t_1, k_2 + t_2, \cdots, k_r + t_r)$, where $(k_1, k_2, \cdots, k_r) \in m_j$ and $(t_1, t_2, \cdots, t_r) \in p_j$. Here s_j is obtained from s'_j exactly as in the definition of the spectral sum.

If I, J are ideals in $\boldsymbol{H}'$ and O, Q their respective cospectra, then the *cospectral intersection* $O \cap Q$, the *cospectral sum* $O + Q$, and the cospectral product OQ are defined in exactly the same manner.

PROPOSITION 3. *Let V and W be varieties and M, P their respective spectra. Then the spectrum of $V \cap W$ is just $M \cap P$. Let I, J be ideals in*

$\boldsymbol{H}'$ and O, Q their cospectra. Then the cospectrum of $I+J$ is $O \cap Q$ and the cospectrum of IJ is OQ.

Proof. The first part is obvious and the second part then follows by Proposition 2. The third part follows easily from the definitions and the product formula for differentiation.

The question naturally arises as to whether the spectrum of $V+W$ is $M+P$, or, what is the same thing, if the cospectrum of $I \cap J$ is $O+Q$. In case that $n=1$, this question has been answered in the affirmative by L. Schwartz (see [12]). We shall discuss the general case presently.

From Proposition 3 we deduce immediately

COROLLARY. *For any ideals I, J in $\boldsymbol{H}'$, the cospectrum of IJ contains that of I. In particular, if $f \in \boldsymbol{H}'$, then the cospectrum of fI contains that of I.*

We shall now formulate the main problems of the theory of mean-periodic functions:

Problem 1. Does every variety contain an exponential? Or, does every ideal in $\boldsymbol{H}'$ have a zero?

Problem 2. Is every variety determined by its exponential polynomials, that is, if W is a variety and $f \in W$, if f the limit of exponential polynomials of W? Equivalently, if I is an ideal in $\boldsymbol{H}'$ and if $f \in \boldsymbol{H}'$ has the property that the cospectrum of f contains that of I, is $f \in I$? (The cospectrum of a $g \in \boldsymbol{H}'$ is the cospectrum of the principal ideal generated by g.)

Problem 3. If V, W are varieties and M, P their respective spectra, is the spectrum of $V+W$ equal to $M+P$? That is, if I and J are ideals in $\boldsymbol{H}'$ and if their respective cospectra are N and O, is $N+O$ the cospectrum of $I \cap J$?

Problem 4. What conditions must the spectrum of a variety satisfy?

Problem 5. If W is a variety, does there exist a single $f \in W$ such that W is the variety generated by f?

Problem 6. Is every ideal in $\boldsymbol{H}'$ finitely generated?

In case $n=1$, Problems 1, 2, 3, 5, and 6 were answered in the affirmative by L. Schwartz in [12]. The solution to Problem 4 in that case is an immediate consequence of the results of that paper: Let $\{(z_j, n_j)\} = R$ be a sequence of tuples, where the z_j are distinct complex numbers with no limit point and the n_j are integers. Let $\{a_k\}$ be an enumeration of the complex numbers z_j,

where each z_j appears n_j times in $\{a_k\}$, and where $|a_k| \leqq |a_{k+1}|$ for all k. A necessary and sufficient condition the R be the spectrum of a variety is that

$$\limsup |a_k|/k < \infty. \tag{12}$$

For, if R is the cospectrum of an ideal in $\boldsymbol{H}'$, then there is an entire function of exponential type which vanishes at each z_j with order n_j; thus, condition (12) holds. On the other hand, if condition (12) holds, then the function $f(z) = z^p \prod_{a_j \neq 0} (1 - z^2/a_j^2)$ is an entire function of exponential type (where p is the number of $a_j = 0$). R is then the cospectrum of the ideal generated by the functions

$$f_k(z) = z^p (z_k - z)^{n_k} \prod_{a_j \neq 0, a_j \neq z_k} (1 - z^2/a_j^2).$$

For general n, a problem analogous to Problem 4, but for rings of indefinitely differentiable functions instead of $\boldsymbol{H}'$, was discussed by H. Whitney in [18], but even in that case the results are only very sketchy

Assume now that the answer to Problem 2 is in the affirmative, and let W be a variety. Let $\{P_k\}$ denote an enumeration of the monomials in n variables. For each k, consider the set Q_k of points a such that $P_k \exp(a\cdot) \in W$. We claim that each Q_k is closed in C. For, if I denotes the Fourier transform of the annihilator ideal of W then, by Proposition 9 of Section 2, there is a partial differential operator D_k such that Q_k may be described as the set of points ib where b is a common zero of all functions $D_k g$ for $g \in I$.

For each k, let $\{c_j^k\}$ be a sequence of points in Q_k whose closure is Q_k. We enumerate all the points c_j^k in some sequence and, for each j, k, we choose a complex number d_j^k in such a manner that the series $\sum d_j^k \exp(c_j^k z) P_k(z)$ converge uniformly for z in any compact set of C and so define an entire function $f \in W$.

It seems reasonable to exepect that the variety generated by f contains all the functions $\exp(c_j^k \cdot) P_k$, so that, by our assumption, the variety generated by f would be W. However, we are not able to demonstrate this fact, which would imply that every variety is generated by a single element (Problem 5).

Concerning Problem 3, it is clear that $M + P$ is contained in the spectrum of $V + W$. Call I, J the Fourier Transforms of the respective annihilator ideals of V, W. By Proposition 1 the Fourier transform of the annihilator ideal of $V + W$ is $I \cap J \supset IJ$. Now IJ is clearly not reduced to zero so that $V + W \neq \mathfrak{A}$.

Assume now that the solution to Problem 1 is in the affirmative. Then

the exponential polynomials of $V+W$ are just the limits of the linear combinations of the exponential polynomials of V and W. We do not know whether the solution to Problem 3 is in the affirmative even in this case.

In what follows we shall solve Problem 2 in case that I is a principal ideal. We shall also give a more simple solution to Problems 1-6 in case that $n=1$ than that given by Schwartz in [12].

4. Solution of the main problem. In order to solve the main problem (Problem 2), we shall make use of the following extension of the Weierstrass preparation theorem (see [2]):

THEOREM 1. *Let P be a function of the complex variables $w, z_1, z_2, \cdots, z_k, x_1, x_2, \cdots, x_r$, which is analytic at the origin, let*

$$D = \partial^{p_1+p_2+\cdots+p_k}/\partial z_1^{p_1}\partial z_2^{p_2}\cdots\partial z_k^{p_k}$$

be a partial differential operator and let s be a positive integer with the following properties:

1. $P(0)=0$.

2. *If E is any partial differential operator in the letters $w, z_1, \cdots, z_k$, but for which at least one of these variables is omitted, then $(EP)(0)=0$.*

3. *The numbers $p_1, p_2, \cdots, p_k, p_{k+1}=s$ are defined as follows:*

(a) *If $q_1<p_1$ and $q_2, q_3, \cdots, q_{k+1}$ are any integers, then*

$$[(\partial^{q_1+q_2+\cdots+q_{k+1}}/\partial z_1^{q_1}\partial z_2^{q_2}\cdots\partial z_k^{q_k}\partial w^{q_{k+1}})P](0)=0.$$

(This defines p_1 uniquely.)

(b) *Suppose $p_1, p_2, \cdots, p_j$ have been defined. Then p_{j+1} is defined by the condition that, if $q_{j+1}<p_{j+1}$ and $q_{j+2}, \cdots, q_{k+1}$ are any integers, then*

$$[(\partial^{p_1+p_2+\cdots+p_j+q_{j+1}+\cdots+q_{k+1}}/\partial z_1^{p_1}\partial z_2^{p_2}\cdots\partial z_j^{p_j}\partial z_{j+1}^{q_{j+1}}\cdots\partial z_k^{q_k}\partial w^{q_{k+1}})P](0)=0.$$

(c) $$(\partial^s DP/\partial w^s)(0)=1.$$

(Thus, the numbers p_j are all defined.)

Then for any function B of $w, z_1, \cdots, z_k, x_1, \cdots, x_r$ which is analytic at the origin there is a unique function Q, analytic at the origin, such that $D(QP)-B$ is, when considered as a power series in w with coefficients functions of $z_1, \cdots, z_k, x_1, \cdots, x_r$ which are analytic at the origin, a polynomial of degree $<s$.

Remark 1. It is allowed that $k=0$, or $r=0$. In case $k=0$, our theorem reduces to the classical Weierstrass preparation theorem.

Remark 2. If P is any function which is analytic at the origin and satisfies $P(0)=0$, then we can find an operator D such that the hypotheses of Theorem 1 are satisfied. For, let P be an analytic function of the complex variables $t_1, t_2, \cdots, t_{r+k+1}$. Call $k+1$ the smallest integer such that there exists a partial differential operator E involving $k+1$ of the variables (say $t_1, t_2, \cdots, t_{k+1}$) with $(EP)(0) \neq 0$. Call $t_1 = z_1$, $t_2 = z_2, \cdots, t_k = z_k$, $t_{k+1} = w$, $t_{k+2} = x_1, \cdots, t_{r+k+1} = x_r$; the integers $p_1, p_2, \cdots, p_k, s$ are then defined by part 3 of the hypotheses of Theorem 1.

Proof of Theorem 1. Write $P = \sum P_u w^u$ where P_u are analytic functions, at zero, of z_j, x_j. For each u, let

$$P_u = \sum P_{uv_1v_2\ldots v_kv_{k+1}} z_1^{v_1} z_2^{v_2} \cdots z_k^{v_k},$$

where $P_{uv_1v_2\ldots v_kv_{k+1}}$ is the homogeneous term of order v_{k+1} in the expansion of P_u as a power series in the x_j

By the product rule for differentiation, we may write

$$D(QP) = PDQ + \cdots + QDP.$$

We denote the general term in the above sum by $P''Q'$, and we write

$$P'' = \sum P''_u w^u, \qquad P''_u = \sum P''_{uv_1\ldots v_{k+1}} z_1^{v_1} \cdots z_k^{v_k},$$

with a similar notation for Q', B, etc.

We are trying to satisfy the equations

$$[D(QP)]_m - B_m = 0 \text{ for } m \geqq s,$$

or, what is the same thing,

$$[D(QP)]_{mv_1\ldots v_{k+1}} - B_{mv_1\ldots v_{k+1}} = 0,$$

whenever $m \geqq s$ and $v_1, v_2, \cdots, v_{k+1} \geqq 0$. Now, $[D(QP)]_{mv_1\ldots v_{k+1}}$ is a sum of terms of the form

$$(Q'P'')_{mv_1\ldots v_{k+1}} = \sum_{u=0}^{m} \sum_{n_1=0}^{v_1} \cdots \sum_{n_{k+2}=0}^{v_{k+1}} Q'_{un_1\ldots n_{k+1}} P''_{m-u, v_1-n_1, \ldots, v_{k+1}-n_{k+1}}.$$

From our hypotheses, we get

(a) For $P'' \neq DP$, $P''_{u0\ldots0} = 0$ for all u.

(b) $DP_{u0\ldots0} = 0$ for $u < s$ and $DP_{s0\ldots0} = 1$.

Thus,

$$[D(QP)]_{mn_1n_2\ldots n_{k+1}} = A + (QDP)_{mn_1\ldots n_{k+1}},$$

where

$$A = \sum_{P'' \neq DP} \sum_{i=1}^{k+1} \sum_{u=0}^{m} \sum_{v_1=0}^{n_1} \cdots \sum_{v_i=0}^{n_i-1} \cdots \sum_{v_{k+1}=0}^{n_{k+1}} (Q'_{uv_1 \ldots v_{k+1}} P''_{m-u, n_1-v_1, \ldots, n_{k+1}-v_{k+1}}).$$

(We shall understand that $\sum_{j=0}^{-1} a_j = 0$.) Now, we may write

$$(QDP)_{mn_1 \ldots n_{k+1}} = E + \sum_{u=0}^{m} Q_{un_1 \ldots n_{k+1}} DP_{m-u, 0 \ldots 0},$$

where

$$E = \sum_{i=1}^{k+1} \sum_{u=0}^{m} \sum_{v_1=0}^{n_1} \cdots \sum_{v_i=0}^{n_i-1} \cdots \sum_{v_{k+1}=0}^{n_{k+1}} (Q_{uv_1 \ldots v_{k+1}} DP_{m-u, n_1-v_1, \ldots, n_{k+1}-v_{k+1}}).$$

We have

$$\sum_{u=0}^{m} Q_{un_1 \ldots n_{k+1}} DP_{m-u, 0 \ldots 0} = \sum_{u=0}^{m-s-1} Q_{un_1 \ldots n_{k+1}} DP_{m-u, 0 \ldots 0} + Q_{m-s, n_1, \ldots, n_{k+1}}$$

$$= G + Q_{m-s, n_1 \ldots n_{k+1}} \text{ say.}$$

Thus, in order to satisfy the equations

$$[D(QP)]_{mn_1 \ldots n_{k+1}} - B_{mn_1 \ldots n_{k+1}} = 0$$

for $m \geqq s, n_1, n_2, \cdots, n_{k+1} \geqq 0$, we must have

$$Q_{m-s, n_1, \ldots, n_{k+1}} = B_{mn_1 \ldots n_{k+1}} - A - E - G.$$

Or, replacing m by $m + s$ in the above, the equations to be satisfied are

$$Q_{mn_1 \ldots n_{k+1}} = B_{m+s, n_1 \ldots n_{k+1}} - A' - E' - G', \tag{1}$$

where A' is obtained from A by replacing m by $m + s$, and E', G' are obtained similarly from E, G respectively.

For any $m, n_1, \cdots, n_{k+1}$, we define

$$g(m, n_1, \cdots, n_{k+1}) = m + \sum_{i=1}^{k} c_i n_{k-i+1} + c_{k+1} n_{k+1}, \tag{2}$$

where the c_j are defined by

$$c_1 = 1 + s;$$

suppose $c_1, \cdots, c_{j-1}$ have been defined, then

$$c_j = 1 + s + \sum_{i=1}^{j-1} c_i p_{k+1-i}.$$

The proof that equations (1) are solvable will be by induction on $g(m, n_1, \cdots, n_{k+1})$. If $g(m, n_1, \cdots, n_{k+1}) = 0$ then $m = 0$ and each $n_j = 0$. Thus, the terms A' and E' are both zero since they involve sums of the form $\sum_{j=1}^{-1}$. Thus, $Q_{0 \ldots 0} = B_{s0 \ldots 0}$.

Assume now that we have proven that equations (1) determine $Q_{uv_1\cdots v_{k+1}}$ uniquely whenever $g(u, v_1, \cdots, v_{k+1}) < g(m, n_1, \cdots, n_{k+1})$. Then, clearly, G' is uniquely determined. On the terms of E', g attains its maximum when, for some $j \leqq k+1$,

$$u = m + s, v_1 = n_1, \cdots, v_{j-1} = n_{j-1}, v_j = n_j - 1, v_{j+1} = n_{j+1}, \cdots, v_{k+1} = n_{k+1}.$$

In that case

$$g(u, v_1, \cdots, v_{k+1}) = m + s + \sum_{i \neq j} c_i n_{k-i+1} + c_{k+1} n_{k+1} + c_j n_{k-j+1} - c_j$$

$$= g(m, n_1, \cdots, n_{k+1}) + s - c_j < g(m, n_1, \cdots, n_{k+1}),$$

because each $c_j \geqq 1 + s$. Thus, E' is also uniquely determined.

Let us write, for $P'' \neq DP$, $Q' = (\partial^{t_1+\cdots+t_k}/\partial z_1^{t_1} \cdots \partial z_k^{t_k})Q$. Then, by the hypotheses of the theorem, $P''_{uv_1\cdots v_k 0} = 0$ if

(a) $v_1 < t_1$ and any $u, v_2, \cdots, v_k$.

(b) $v_1 = t_1, \cdots, v_j = t_j, v_{j+1} < t_{j+1}$, and any $u, v_{j+2}, \cdots, v_k$.

(c) $v_1 = t_1, \cdots, v_k = t_k, u < s$.

Consider the terms $Q'_{uv_1\cdots v_{k+1}}$ in A' (for a fixed P'') for which

(α) $u = m + s, n_1 - v_1 = t_1 + 1, v_2 = n_2, \cdots, v_{k+1} = n_{k+1}$.

(β) $u = m + S, \quad n_1 - v_1 = t_1, \cdots, n_j - v_j = t_j, \quad n_{j+1} - v_{j+1} = t_{j+1} + 1,$
$v_{j+2} = n_{j+2}, \cdots, v_{k+1} = n_{k+1}$.

(γ) $u = m + s, v_1 = n_1, \cdots, v_k = n_k, v_{k+1} = n_{k+1} - 1$.

(δ) $u = m, n_1 - v_1 = t_1, \cdots, n_k - v_k = t_k, v_{k+1} = n_{k+1}$.

(It may happen that some of these terms do not occur, but we shall neglect this fact since it will be seen that, in this case, the equations (1) are certainly solvable.)

Given any term $Q'_{u'v'_1\cdots v'_{k+1}}$ in A' for this same P'', let us notice that this term is uniquely determined by $Q_{u', v'_1+t_1, \cdots, v'_k+t_k, v'_{k+1}}$. From (a), (b), and (c), given any such term for which the subscripts $u', v'_1, \cdots, v'_{k+1}$ do not satisfy any of the conditions (α), (β), (γ), or (δ), we can find a term $Q'_{uv_1\cdots v_{k+1}}$ whose subscripts satisfy one of these conditions, and such that

$$g(u', v'_1 + t_1, \cdots, v'_k + t_k, v'_{k+1}) < g(u, v_1 + t_1, \cdots, v_k + t_k, v_{k+1}).$$

We shall show that in cases (α), (β), and (γ)

$$g(u, v_1 + t_1, \cdots, v_k + t_k, v_{k+1}) < g(m, n_1, \cdots, n_{k+1}).$$

Case (α). We have

$$g(u, v_1 + t_1, \cdots, v_k + t_k, v_{k+1}) \leqq m + s\sum_{i=1}^{k-1} c_i(n_{k-i+1} + p_{k-i+1}) + c_k(n_1 - 1) + c_{k+1}n_{k+1}$$
$$= m + \sum_{i=1}^{k} c_i n_{k-i+1} + c_{k+1}n_{k+1} + s + \sum_{i=1}^{k-1} c_i p_{k-i+1} - c_k$$
$$= g(m, n_1, \cdots, n_{k+1}) - 1.$$

Case (β).

$$g(u, v_1 + t_1, \cdots, v_k + t_k, v_{k+1}) \leqq m + s + c_{k+1}n_{k+1} + \sum_{i=1}^{k-j-1} c_i(n_{k-i+1} + p_{k-i+1}) + c_{k-j}(n_{j+1} - 1) + \sum_{i=k-j+1}^{k} c_i n_{k+1-i}$$
$$= g(m, n_1, \cdots, n_{k+1}) + s + \sum_{i=1}^{k-j-1} c_i p_{k-i+1} - c_{k-j}$$
$$= g(m, n_1, \cdots, n_{k+1}) - 1.$$

Case (γ).

$$g(u, v_1 + t_1, \cdots, v_k + t_k, v_{k+1}) \leqq m + s + \sum_{i=1}^{k} c_i(n_{k-i+1} + p_{k-i+1}) + c_{k+1}(n_{k+1} - 1)$$
$$= g(m, n_1, \cdots, n_{k+1}) - 1.$$

Case (δ). In this case, clearly,

$$g(u, v_1 + t_1, \cdots, v_k + t_k, v_{k+1}) = g(m, n_1, \cdots, n_{k+1}).$$

The term in question is

$$Q'_{m, n_1 - t_1, \ldots, n_k - t_k, n_{k+1}} P''_{s, t_1 \ldots t_k 0} = dQ_{m n_1 \ldots n_{k+1}} P_{s p_1 \ldots p_k 0} = dQ_{m n_1 \ldots n_{k+1}},$$

because $P_{s p_1 \ldots p_k 0} = 1$, where d is some constant $\geqq 0$ (which may depend on P'').

Thus, equation (1) takes the form

$$(3) \qquad (1 + \Sigma d) Q_{m n_1 \ldots n_{k+1}} = B_{m+s, n_1 \ldots n_{k+1}} + R_{m n_1 \ldots n_{k+1}},$$

where $R_{m n_1 \ldots n_{k+1}}$ depends only on those $Q_{u v_1 \ldots v_{k+1}}$ for which

$$g(u, v_1, \cdots, v_{k+1}) < g(m, n_1, \cdots, n_{k+2}).$$

Thus, equation (1) determines the $Q_{m n_1 \ldots n_{k+1}}$ uniquely.

Analyticity of Q. We have shown that Q exists and is unique as a formal power series; we shall now show that this power series converges in the neighborhood of the origin.

We shall produce positive numbers $k, a, a_1, \cdots, a_{k+1}$ all > 2 so that

$$(4) \qquad |Q_{m n_1 n_2 \ldots n_{k+1}}(x)| \leqq K a^m a_1^{n_1} a_2^{n_2} \cdots a_{k+1}^{n_{k+1}}$$

for all x in a suitable neighborhood of zero N in complex Euclidean r-space X. Since nothing is altered in either the hypotheses or conclusion of Theorem 1 upon application of the linear transformation

$$w \to cw, z_1 \to cz_1, \cdots, z_k \to cz_k, x_1 \to cx_1, \cdots, x_r \to cx_r$$

for $c > 0$, we may assume that both B and P are analytic in the unit ball in complex Euclidean $k + r + 1$-space. (The unit ball in C is the set of $z \varepsilon C$ such that $|z| \leqq 1$.) Thus, there exist constants $L > 0$, $M > 0$ so that, for all $m, n_1, \cdots, n_{k+1}$, and all $x \varepsilon X$ with $|x| \leqq 1$, we have

$$|B_{mn_1 \cdots n_{k+1}}(x)| \leqq L, \qquad |P''_{mn_1 \cdots n_{k+1}}(x)| \leqq M,$$

for all P''.

The proof that equation (4) is satisfied will be by induction on $g(m, n_1, \cdots, n_{k+1})$. For N we choose the unit ball in X. Next, choose $K > 2$ so that for all $x \varepsilon N$

$$|Q_{00\cdots0}(x)| \leqq K.$$

(Such a K can be found by virtue of the definition of $Q_{00\cdots0}$.)

Now, assume (4) is satisfied for all $u, v_1, \cdots, v_{k+1}$ such that

$$g(u, v_1, \cdots, v_{k+1}) < g(m, n_1, \cdots, n_{k+1}) > 0.$$

Set

$$G(m, n_1, \cdots, n_{k+1}) = Ka^m {a_1}^{n_1} \cdots {a_{k+1}}^{n_{k+1}}.$$

Let us examine the terms $Q'_{uv_1v_2 \cdots v_{k+1}}$ which appear on the right side of equation (3). Each is a constant multiple of some term $Q_{u'v'_1 \cdots v'_{k+1}}$ with

$$g(u'v'_1 \cdots v'_{k+1}) < g(m, n_1, \cdots, n_{k+1}).$$

Moreover, each of these constant multipliers does not exceed

$$(n_1 + p_1)^{p_1}(n_2 + p_2)^{p_2} \cdots (n_k + p_k)^{p_k}.$$

On the other hand, there is a term d on the left side of equation (3) with

$$d = n_1(n_1 - 1) \cdots (n_1 - p_1)n_2(n_2 - 1) \cdots (n_2 - p_2) \cdots n_k(n_k - 1)(n_k - p_k),$$

where it is understood that, in the above product, each term which is $\leqq 0$ is to be replaced by 1. Thus, the ratio of the maximum constant multiplier on the right side of equation (3) to $1 + \sum d$ does not exceed

$$h = (2p_1)^{p_1}(2p_2)^{p_2} \cdots (2p_k)^{p_k}.$$

Further, no term $Q_{u'v'_1 \cdots v'_{k+1}}$ can be involved on the right side of equation (3) more than

$$q = p_1!\, p_2! \cdots p_k!$$

times.

From the above considerations and equation (3) we have, for any $x \in N$,

$$|Q_{mn_1\dots n_{k+1}}(x)| \leqq L + Mhq \times \Big[\sum_{u=0}^{m+s} \sum_{v_1=0}^{n_1-1} \sum_{v_2=0}^{n_2+p_2} \cdots \sum_{v_k=0}^{n_k+p_k} \sum_{v_{k+1}=0}^{n_{k+1}} G(u, v_1, \cdots, v_{k+1})$$
$$+ \sum_{u=0}^{m+s} \sum_{v_2=0}^{n_2-1} \sum_{v_3=0}^{n_3+p_3} \cdots \sum_{v_k=0}^{n_k+p_k} \sum_{v_{k+1}=0}^{n_{k+1}} G(u, n_1, v_2, \cdots, v_{k+1})$$
$$+ \cdots + \sum_{u=0}^{m+s} \sum_{v_k=1}^{n_k-1} \sum_{v_{k+1}=0}^{n_{k+1}} G(u, n_1, \cdots, n_{k-1}, v_k, v_{k+1})$$
$$+ \sum_{u=0}^{m+s} \sum_{v_{k+1}=0}^{n_{k+1}-1} G(u, n_1, \cdots, n_k, v_{k+1}) + \sum_{u=0}^{m-1} G(u, n_1, \cdots, n_{k+1}) \Big],$$

because of (α), (β), (γ), and (δ) above.

Thus,

$$|Q_{mn_1\dots n_{k+1}}(x)| \leqq L + MKqh \times \Big[\frac{a^m}{a-1} {a_1}^{n_1} \cdots {a_{k+1}}^{n_{k+1}}$$
$$+ a^{m+s+1} {a_1}^{n_1} \cdots {a_k}^{n_k} \frac{{a_{k+1}}^{n_{k+1}}}{a_{k+1}-1}$$
$$+ a^{m+s+1} {a_1}^{n_1} \cdots {a_{k-1}}^{n_{k-1}} \frac{{a_k}^{n_k}}{a_k-1} {a_{k+1}}^{n_{k+1}+1}$$
$$+ a^{m+s+1} {a_1}^{n_1} \cdots {a_{k-2}}^{n_{k-2}} \frac{{a_{k-1}}^{n_{k-1}}}{a_{k-1}-1} {a_k}^{n_k+p_k+1} {a_{k+1}}^{k+1}$$
$$+ \cdots + a^{m+s+1} \frac{{a_1}^{n_1}}{a_1-1} {a_2}^{n_2+p_2+1} {a_k}^{n_k+p_k+1} {a_{k+1}}^{n_{k+1}+1} \Big].$$

We want to make this $\leqq K a^m {a_1}^{n_1} \cdots {a_{k+1}}^{n_{k+1}}$. This will be the case if

$$L + MKhq \times \Big[\frac{1}{a-1} + a^{s+1} \frac{1}{a_{k+1}-1} + a^{s+1} a_{k+1} \frac{1}{a_k-1} + a^{s+1} a_{k+1} a_k^{p_k+1} \frac{1}{a_{k-1}-1}$$
$$+ \cdots + a^{s+1} a_{k+1} a_k^{p_k+1} \cdots + {a_2}^{p_2+1} \frac{1}{a_1-1} \Big] \leqq K.$$

This can be done by choosing successively $a, a_1, \cdots, a_{k+1}$ all > 2 so that each summand above is $\leqq K/(k+2)(L+MKhq)$.

With this choice of $a, a_1, \cdots, a_{k+1}$ the induction process can be completed. Thus relation (4) is satisfied. This means that Q is analytic in a suitable neighborhood of the origin, which concludes the proof of Theorem 2.

Let $a \in C$ and let f, g be functions which are analytic in the neighborhood of a. We shall say that the *cospectrum of f contains the cospectrum of g at a* if there exists a neighborhood N of a so that, for any $b \in N$ and any non-negative integers $t_1, \cdots, t_n$, the conditions

$$[(\partial^{s_1+s_2+\cdots+s_n} / \partial {Z_1}^{s_1} \partial {Z_2}^{s_2} \cdots \partial {Z_n}^{s_n}) g](b) = 0,$$

whenever $s_1 \leqq t_1, s_2 \leqq t_2, \cdots, s_n \leqq t_n$ imply

$$[(\partial^{s_1+s_2+\cdots+s_n}/\partial Z_1^{s_1}\partial Z_2^{s_2}\cdots\partial Z_n^{s_n})f](b) = 0$$

for all $s_1 \leqq t_1, s_2 \leqq t_2, \cdots, s_n \leqq t_n$. In part II of this series we shall discuss in detail the concept of the cospectrum of a local ideal at a (see [3]).

THEOREM 2. *Let $a \in C$ and let P, g be functions which are analytic in a neighborhood of a. Suppose that the cospectrum of g contains the cospectrum of P at a. Then there is a function h analytic at a such that $g = hP$ in a suitable neighborhood of a.*

Proof. The theorem is trivially true in case that $P = 0$, for then we must have $g = 0$; we therefore assume $P \neq 0$. It is clearly no loss in generality to assume that $a = 0$. If $P(0) \neq 0$, then the result is obvious; we assume also that $P(0) = 0$. $D, w, z_1, \cdots, z_k, x_1, \cdots, x_r$ are now defined as in the hypotheses of Theorem 1 $(r + k + 1 = n)$.

By Theorem 1, there is a unique function S analytic at the origin such that

$$D[P(w,z,x)S(w,z,x)] = w^s + \sum_{j=0}^{s-1} K_j(z,x)w^j, \tag{5}$$

where K_j are analytic at the origin. It is shown in the proof of Theorem 1 that $S(0) = S_{0\ldots0} = 1$. Thus, the operator D and the function PS also satisfy the hypotheses of Theorem 1. Hence, by Theorem 1, we can find a function Q analytic at the origin and such that

$$D[P(w,z,x)S(w,z,x)Q(w,z,x)] - Dg(w,z,x) = \sum_{j=0}^{s-1} H_j(z,x)w^j, \tag{6}$$

where the H_j are analytic at the origin.

Let M be a ball in C of radius so small that all functions which appear in equations (5) and (6) are analytic in M, and such that $S \neq 0$ in M. Then we integrate equations (5) and (6) p_1 times with respect to z_1, p_2 times with respect to $z_2, \cdots$, p_k times with respect to z_k, where all paths of integration begin at the origin and lie entirely in M. Then we obtain

$$P(w,z,x)S(w,z,x) = \sum_{j=0}^{s} \tilde{K}_j(z,x)w^j, \tag{7}$$

$$P(w,z,x)S(w,z,x)Q(w,z,x) - g(w,z,x) = \sum_{j=0}^{s-1} \tilde{H}_j(z,x)w^j. \tag{8}$$

Let us note that $K_j(0,0) = 0$ for $j = 0, 1, \cdots, s-1$. For, were this not the case, the integer s would not have required minimum property of the

hypotheses of Theorem 1. It is fairly easy to see, moreover, using the properties of the operator D, that, for each $j < s$,

$$\lim_{z\to 0,\ x\to 0} \tilde{K}_j(z,x)/\tilde{K}_s(z,x) = 0.$$

By hypothesis, the cospectrum of g contains the cospectrum of P at 0; since $S(0) \neq 0$, the cospectrum of g contains the cospectrum of PS at 0. Thus, there exists a neighborhood of zero $N \subset M$ so that, for any $b \in N$ and any integers $t_1, \cdots, t_n$, the conditions

$$[(\partial^{s_1+\cdots+s_n}/\partial Z_1^{s_1} \cdots \partial Z_n^{s_n})PS](b) = 0,$$

for $s_1 \leqq t_1, \cdots, s_n \leqq t_n$, imply

$$[(\partial^{s_1+\cdots+s_n}/\partial Z_1^{s_1} \cdots \partial Z_n^{s_n})g](b) = 0,$$

whenever $s_1 \leqq t_1, \cdots, s_n \leqq t_n$.

Now, for $a_0 \neq 0$, the zeros of the polynomial $a_0X^t + a_1X^{t-1} + \cdots + a_t$ depend continuously on $(a_1/a_0, a_2/a_0, \cdots, a_t/a_0)$. Thus, by the above, we may choose a point (z_0, x_0) such that $K_s(z_0, x_0) \neq 0$ and such that all the zeros c of $\sum_{j=0}^{s} \tilde{K}_j(z_0, x_0)w^j$ have the property that (c, z_0, x_0) lies in N.

We wish to show that all $\tilde{H}_j = 0$. Assume this is not the case; then we may assume that (z_0, x_0) is so chosen that $\tilde{H}_t(z_0, x_0) \neq 0$ for some t.

It follows from the above that if $(b, z_0, x_0) \in N$ has the property that b is a k-fold zero of $\sum_{j=0}^{s} \tilde{K}_j(z_0, x_0)w^j$, then b is also (at least) a k-fold zero of $\sum_{j=0}^{s-1} \tilde{H}_j(z_0, x_0)w^j$. But, we have seen that $\sum_{j=0}^{s} \tilde{K}_j(z_0, x_0)w^j$ has s zeros $b_1, \cdots, b_s$ counting multiplicity, with $(b_j, z_0, x_0) \in N$ for all j. Thus $\sum_{j=0}^{s-1} \tilde{H}_j(z_0, x_0)w^j$ has at least s zeros. This can only be the case if all $\tilde{H}_j(z_0, x_0) = 0$. This contradiction concludes the proof of Theorem 2.

We have the immediate

COROLLARY. *Let $a \in C$, f, g be functions which are analytic at a and such that the cospectrum of f contains the cospectrum of g at a. Let L be a linear transformation of $C \to C$. Then the cospectrum of fL contains the cospectrum of gL at La.*

Remark. If a proof of this corollary could be found which is independent of Theorems 1 and 2, then this corollary, together with the Weierstrass preparation theorem, could be used to give a simplified proof of Theorem 2 without the use of Theorem 1.

Let f, g be entire functions on C. We shall say that *the cospectrum of f contains the cospectrum of g* if, for any $a \in C$, the cospectrum of f contains the cospectrum of g at a. It is clear that, if f and g are of exponential type, this definition coincides with the previous one (see Section 3).

THEOREM 3. *Let f, g be entire functions such that the cospectrum of f contains the cospectrum of g. Then there is an entire function h such that $f = gh$.*

Proof. f/g is clearly analytic outside of the set of zeros of g. According to the theorem of removable singularities (see [2]), it is sufficient to prove that f/g is bounded in the neighborhood of each point. This is an immediate consequence of Theorem 2.

The passage from arbitrary entire functions to entire functions of exponential type is accomplished by Theorem 4 below; for $n = 1$, Theorem 4 is a result of E. Lindelöf (see [10]).

THEOREM 4. *Let f, g, h be entire functions of n complex variables, with $g = fh \neq 0$. Suppose that f and g are of exponential type. Then h is also of exponential type.*

The following minimum modulus theorem, which is itself of interest, is the key tool in the proof of Theorem 4:

THEOREM 5. *Let k be an entire function of exponential type of one complex variable with $k(0) \neq 0$ and $|k(z)| \leqq Me^{\exp(A|z|)}$, for all z. Then for any $r > 0$ there is an r' with $r \leqq r' \leqq 2r$ such that*

$$\min_{|z|=r'} |k(z)| \geqq \exp(B \log M + cAr' + d \log |k(0)|)$$

where B and c are certain constants, and where d is a positive integer.

Let us assume the truth of Theorem 5 and conclude the proof of Theorem 4. We shall prove by induction on p the following proposition α_p: Let H, K be constants, $f \neq 0$ an entire function of exponential type of p variables, and h an entire function on C $(p \leqq n)$ such that, for any $(z_1, \cdots, z_n) \in C$,

$$|f(z_1, \cdots, z_p)|\,|h(z_1, \cdots, z_n)| \leqq K \exp(H \|z\|).$$

Then h is of exponential type.

Now, α_0 is trivially true, because for $p = 0$, f is a constant $\neq 0$. Let $p > 0$ and assume α_q is true whenever $q < p$. Suppose that $|f(z'_1, z'_2, \cdots, z'_p)| \leqq L \exp[N(|z'_1| + \cdots + |z'_v|)]$ for all $(z'_1, \cdots, z'_p)$. Let $(z_1, \cdots, z_n)$

be any point in C such that $f(0, z_2, \cdots, z_p) \neq 0$, and also $z_1 \neq 0$. By Theorem 5 we can find an r' with $|z_1| \leqq r' \leqq 2|z_1|$ such that

$$\min_{|z|=r'} |f(z, z_2, \cdots, z_p)| \geqq L^B |f(0, z_2, \cdots, z_p)|^d \exp[BN(|z_2| + \cdots + |z_p|) + cNr'],$$

where B, c, and d are certain constants. (Because $z \to f(z, z_2, \cdots, z_p)$ is an entire function of exponential type of one complex variable which is different from zero at the origin.)

From this it follows that, for any z with $|z| = r'$,

$$\begin{aligned} L^B |f(0, z_2, \cdots, z_p)|^d \exp(BN(|z_2| + \cdots + |z_p|) + cNr') |h(z, z_2, \cdots, z_n)| \\ \leqq |f(z, z_2, \cdots, z_p)| \, |h(z, z_2, \cdots, z_n)| \\ \leqq K e^{H(|z|+|z_2|+\cdots+|z_n|)}. \end{aligned}$$

Thus,

$$\begin{aligned} |f(0, z_2, \cdots, z_p)|^d |h(z, z_2, \cdots, z_n)| \\ \leqq KL^{-B} \exp((H - BN)(|z_2| + \cdots + |z_n|) + (H - cN)r') \\ \leqq KL^{-B} \exp((H - BN)(|z_2| + \cdots + |z_n|) + 2(H - cN)|z_n|), \end{aligned}$$

because $r' \leqq 2|z|$. Hence, by the maximum modulus theorem

$$\begin{aligned} |f(0, z_2, \cdots, z_p)|^d |h(z_1, z_2, \cdots, z_n)| \\ \leqq KL^{-B} \exp(H - BN)(|z_2| + \cdots + |z_n|) + 2(H - cN)|z_1|). \end{aligned}$$

This inequality holds for all $(z_1, \cdots, z_n)$ such that $z_1 \neq 0$ and $f(0, z_2, \cdots, z_p) \neq 0$; by continuity it holds without these restrictions.

Now, $(z_2, \cdots, z_p) \to f(0, z_2, \cdots, z_p)$ is an entire function of exponential type in $p - 1$ variables. Thus, by our induction hypothesis, h is an entire function of exponential type, i.e., Proposition α_p is established. This completes our induction; Theorem 4 results immediately.

Proof of Theorem 5. We claim it is sufficient to consider the case in which k is an even function. For, assume Theorem 5 is proven for even functions and set $f = k\check{k}$, where $\check{k}(x) = k(-x)$, so f is an even entire function of exponential type. Suppose that $|k(z)| \leqq M e^{A|z|}$, so that $|f(z)| \leqq M^2 e^{2A|z|}$ for all complex numbers z. Then, by the assumed result for even functions, given $r > 0$ we can find an r' with $r \leqq r' \leqq 2r$ such that

$$\min_{|z|=r'} |f(z)| \geqq \exp(2B \log M + 2cA|z| + d \log |f(0)|),$$

for some constants B, c, and d.

Let z_0 be a point on $|z| = r'$ at which $|k|$ attains its minimum. Then

$$|f(z_0)| = |k(z_0)|\,|k(-z_0)| \leqq |k(z_0)| \max_{|z|=r'} |k(z)|.$$

Thus,

$$\min_{|z|=r'} |f(z)| \leqq |k(z_0)| \max_{|z|=r'} |k(z)|$$

$$= \min_{|z|=r'} |k(z)| \max_{|z|=r'} |k(z)| \leqq Me^{Ar'} \min_{|z|=r'} |k(z)|.$$

We conclude that

$$\min_{|z|=r'} |k(z)| \geqq M^{-1}e^{-Ar'} \min_{|z|=r'} |f(z)|$$

$$\geqq \exp[(2B-I)\log M + (2c-1)Ar' + 2d \log |k(0)|],$$

which is the desired inequality.

Theorem 5 results immediately from the above and

THEOREM 6. *Let k be an entire function of finite order of one complex variable with $k(0) \neq 0$. Call p the genus of k and assume that k is invariant under the linear transformation $z \to \omega z$ of the complex plane into itself, where ω is a primitive $(p+2)$-nd root of unity. Then for any $r > 0$ there is an r' with $r \leqq r' \leqq 2r$ such that*

$$\min_{|z|=r'} |k(z)| \geqq 2\,|k(0)|^{11} \exp[-2\sum_{j=0}^{\infty} 2^{-j(p+2)}(2^{p+2}-1)\log M(2^{j+3}r)],$$

where, for any $y > 0$, $M(y) = \max_{|z|=y} |k(z)|$.

Proof of Theorem 6. From the fact that, for any $k < p+2$, $\sum_{j=1}^{p+2} \omega^{kj} = 0$, we deduce easily that the Weierstrass-Hadamard product for k (see [16]) takes the form $k(z) = \delta \prod (1 - z^{p+2}/a_j^{p+2})$, where $\delta = k(0)$.

We write $k(z) = \delta\pi_1(z)\pi_2(z)\pi_3(z)$ where

$\pi_1(z)$ consists of all terms of $\prod$ for which $|a_j| \leqq r/2$,

$\pi_2(z)$ consists of all terms of $\prod$ for which $r/2 < |a_j| \leqq 4r$,

$\pi_3(z)$ consists of all terms of $\prod$ for which $|a_j| > 4r$.

(By convention, an empty product is to be replaced by unity.)

For π_1 we use the trivial estimate that, for $|z| \geqq r$,

$$|1 - z^{p+2}/a_j^{p+2}| \geqq |z/a_j|^{p+2} - 1 \geqq 2^{p+2} - 1 > 1,$$

so that $|\pi_1(z)| \geqq 1$ whenever $|z| \geqq r$.

For π_2 and π_3 we shall need Jensen's formula (see [16]). If $m(x)$ denotes the number of zeros of k of modulus $\leqq x$, then for any $y > 0$,

$$\int_0^y (m(x)/x)dx = (1/2\pi)\int_0^{2\pi} \log k(ye^{i\theta})d\theta - \log|k(0)| \leqq \log M(y) - \log|\delta|.$$

But, m is a non-decreasing function, so

$$2\int_y^{2y} (m(x)/x)dx \geqq m(y)2\int_y^{2y} dx/x \geqq m(y).$$

Hence,

$$\tfrac{1}{2}m(y) \leqq \int_0^{2y} (m(x)/x)dx \leqq \log M(2y) - \log|\delta|. \tag{10}$$

From (10) we see that in π_2 there are not more than

$$\beta = (2/p+2)(\log M(8r) - \log|\delta|) \text{ terms } a_j.$$

Now (see [11], p. 86, problem 66) we can find an r' such that $r \leqq r' \leqq 2r$ and such that

$$\prod_{a_j \in \pi_2} |(|a_j| - r')| \geqq 2(r/4)^{\beta}. \tag{11}$$

Also, if $|z| = r'$,

$$\begin{aligned} &|a_j^{p+2} - z^{p+2}| \\ &= (a_j - z)(a_j - \omega z) - \cdots - (a_j - \omega^{p+1}z) \geqq |(|a_j| - r')|^{p+2}. \end{aligned} \tag{12}$$

Thus, if $|z| = r'$,

$$\begin{aligned} \prod_{a_j \in \pi_2} |1 + z^{p+2}/a_j^{p+2}| &\geqq (4r)^{-\beta(p+2)} \prod_{a_j \in \pi_2} |a_j^{p+2} - z^{p+2}| \\ &\geqq (4r)^{-\beta(p+2)} \prod_{a_j \in \pi_2} |(|a_j| - r')|^{p+2} \\ &\geqq (4r)^{-\beta(p+2)} 2(r/4)^{\beta(p+2)} \geqq 2(4)^{-2\beta(p+2)}, \end{aligned}$$

by (11) and (12); that is, $|\pi_2(z)| \geqq 2(4)^{-2\beta(p+2)}$ for $|z| = r'$. It is clear that this implies

$$|\pi_2(z)| \geqq 2|\delta|^8 \exp(-4\log M(8r)). \tag{13}$$

For π_3 we use the estimate

$$|1 - z^{p+2}/a_j^{p+2}| \geqq 1 - |z/a_j|^{p+2} \geqq \exp(-|z/a_j|^{p+2}). \tag{14}$$

This results from the fact that, for $0 < u < \frac{1}{2}$,

$$\log(1-u) = -u - u^2/2 - u^3/3 - \cdots > -u,$$

so that $1 - u > \exp(-u)$.

For any $j \geqq 2$, consider the annulus $R_j: 2^j r < z \leqq 2^{j+1}r$. In R_j there are not more than $\beta_j = (2/p+2)(\log M(2^{j+2}r) - \log|\delta|)$ terms a_j by (10). For each of them,

$$|r'/a_j| \leqq 2r/2^j r = 2^{1-j}. \tag{15}$$

Thus, if $|z| = r'$, using (14) and (15),

$$|\pi_3(z)| \geqq \exp(-\sum |r'/a_j|^{p+2}) \geqq \exp(-\sum_{j=2}^{\infty} (p+2)\beta_j 2^{(p+2)(1-j)}).$$

Now, $\sum_{j=2}^{\infty} 2^{(p+2)(1-j)} = 1/2^{p+2} - 1 < 1$. Thus,

$$(16) \qquad |\pi_3(z)| \geqq \exp(-2^{p+2}-1) \sum_{j=2}^{\infty} (p+2)\beta_j 2^{(p+2)(1-j)}$$

$$= |\delta|^2 \exp[-2 \sum_{j=2}^{\infty} 2^{(p+2)(1-j)}(2^{p+2}-1)\log M(2^{j+2}r)],$$

for all z with $|z| = r'$. Putting all our estimates together, we have

$$\min_{z=r'} |k(z)| \geqq |\delta| \min_{z=r'} |\pi_1(z)| \min_{z=r'} |\pi_2(z)| \min_{z=r'} |\pi_3(z)|$$

$$\geqq 2\,|k(0)|^{11} \exp[-\sum_{j=0}^{\infty} 2^{-(p+2)j}(2^{p+2}-1)\log M(2^{j+3}r)],$$

which is the desired result.

Combining Theorems 3 and 4 we have

THEOREM 7. *Every principal ideal in $\boldsymbol{H}'$ is completely determined by its cospectrum, that is, if $f, g \in \boldsymbol{H}'$ and if the cospectrum of g contains the cospectrum of f, then g lies in the ideal generated by f in $\boldsymbol{H}'$.*

THEOREM 8. *Let $f \in \boldsymbol{H}'$ and let $I = \{fh\}_{h \in \boldsymbol{H}'}$. Then I is closed, i.e., every principal algebraic ideal in $\boldsymbol{H}'$ is an ideal in $\boldsymbol{H}'$.*

Proof. Let g be in the closure of I; it is clear that the cospectrum of g contains the cospectrum of f. Thus, by Theorems 3 and 4, $g \in I$.

Remark. It is easily seen that the set I above is even closed in $\mathfrak{A}$, and hence weakly in $\boldsymbol{H}'$ (that is, if $\boldsymbol{H}'$ is given the weak topology of the dual of $\boldsymbol{H}'$).

From Theorem 7 and the results of Section 3 we deduce

THEOREM 9. *Let V be a variety whose annihilator ideal is principal. Then V contains an exponential polynomial. Moreover, V is completely determined by its exponential polynomials, that is, every $f \in V$ is the limit of exponential polynomials of V.*

Theorem 9 is the generalization to n variables of the theorem of Ritt, Valiron, and others to the effect that every solution of a differential equation of infinite order with constant coefficients is the limit of exponential polynomial solutions of the equation (see [12]).

5. Extension to other spaces. In this section, we shall investigate rings $\mathfrak{O}$ of entire functions with the following property: Let $f, g \in \mathfrak{O}$ and suppose that the cospectrum of g contains the cospectrum of f. Then there is an $h \in \mathfrak{O}$ such that $g = fh$. Theorem 2 of Section 4 tells us that, for any $a \in C$, if $\mathfrak{P}_a$ denotes the ring of functions analytic at a, then every principal ideal in $\mathfrak{P}_a$ is determined by its cospectrum at a (that is, if $F, G \in \mathfrak{P}_a$ and if the cospectrum of G contains the cospectrum of F at a, then $G = FH$ for some $H \in \mathfrak{P}_a$). Thus, the above property of $\mathfrak{O}$ can be reformulated as follows: Every principal ideal in $\mathfrak{O}$ is determined by its local ideals, that is, by the ideals it generates in $\mathfrak{P}_a$ for all $a \in C$ (see [3]). Theorems 3 and 4 of Section 4 show that we may take for $\mathfrak{O}$ the ring of entire functions or the ring of entire functions of exponential type. In this section we shall show that we may take for $\mathfrak{O}$ the ring of polynomials or, for any $c \geqq 0$, the ring of entire functions of order $\leqq c$, hence also the ring of all entire functions of finite order, and more general rings.

THEOREM 1. *Every principal ideal in the ring of polynomials is determined by its local ideals. Equivalently, if P is any polynomial and Q a polynomial whose cospectrum contains the cospectrum of P, then $Q = PS$ for some polynomial S.*

Proof. According to Theorem 3 of Section 4, we must show the following: Let f and g be polynomials in n letters with $f \neq 0$ and let h be an entire function of n complex variables such that $g = fh$; then h is also a polynomial. The proof will be by induction on p of the following proposition: Let $f \neq 0$ be a polynomial in p letters ($p \leqq n$) and h an entire function of n complex variables such that, for all $(z_1, \cdots, z_n) \in C$,

$$|f(z_1, \cdots, z_p)h(z_1, \cdots, z_n)| \leqq (1 + |z_1| + \cdots + |z_n|)^k,$$

for some $k \geqq 0$. Then h is a polynomial.

For $p = 0$, f is a non-zero constant and the result is immediate. Assume $p > 0$ and that the result is true for polynomials in fewer than p letters. Let $(z_1, \cdots, z_n) \in C$, and write

$$f(X_1, X_2, \cdots, X_p) = f_0 X_1^q + f_1 X_1^{q-1} + \cdots + f_q,$$

where the f_j are polynomials in $X_2, \cdots, X_p$ and where $f_0 \neq 0$. By the results of [9], we can describe a circle γ of radius $\leqq 1$ about z_1 so that, for all $z \in \gamma$,

$$|f(z, z_2, \cdots, z_p)| \geqq \beta\, |f_0(z_2, \cdots, z_p)|,$$

where β is a positive constant which depends only on the degree of f. Thus, for any $z \in \gamma$,

$$\begin{aligned}|\beta f_0(z_2,\cdots,z_p)h(z,z_2,\cdots,z_n)| &\leqq |f(z,z_2,\cdots,z_p)h(z,z_2,\cdots,z_n)| \\ &\leqq (1+|z|+|z_2|+\cdots+|z_n|)^k \\ &\leqq (2+|z_1|+|z_2|+\cdots+|z_n|)^k \\ &\leqq 2^k(1+|z_1|+\cdots+|z_n|)^k.\end{aligned}$$

Hence, by the maximum modulus theorem,

$$|2^{-k}\beta f_0(z_2,\cdots,z_p)h(z_1,z_2,\cdots,z_n)| \leqq (1+|z_1|+\cdots+z_n|)^k.$$

Now, $2^{-k}\beta f_0$ is a polynomial in fewer than p variables. Thus, by our induction assumption, h is a polynomial. Theorem 1 now results immediately.

Let $f \not\equiv 0$ be an entire function of n complex variables. We say that f is of finite order if there is an $A \geqq 0$ so that

$$|f(z)| = O(\exp(\|z\|^A)). \tag{1}$$

The greatest lower bound of all numbers A which satisfy (1) is called the order of f. In order to prove the analog of Theorem 1 for the ring of entire functions of finite order, we shall need the following form of the minimum modulus theorem (see [16])

THEOREM 2. *Let f be an entire function of one complex variable, with $|f(z)| \leqq M\exp(.z|^A)$, and such that $f(0) \neq 0$. Then for any $r > 0$ there is an r' with $r \leqq r' \leqq 2r$ and*

$$\min_{|z|=r'} |f(z)| \geqq \exp(\alpha \log M + \zeta |z|^A + \gamma \log |f(0)|),$$

where α, ζ, and γ are constants which depend only on A, and where we may choose, for γ, a positive integer.

Proof. Call p the genus of f (see [16]). Then, as in the proof of Theorem 5 of Section 4, it is sufficient to consider the case in which f is invariant under the linear transformation $z \to wz$ of the complex plane into itself, where w is a primitive $(p+2)$-nd root of unity. The result now follows immediately from Theorem 6 of Section 4.

Exactly as in the proof of Theorem 4 of Section 4 (except that we use Theorem 3 instead of Theorem 5 of Section 4), we deduce

THEOREM 4. *For any $A > 0$, denote by Ω_A the ring of entire functions of order $\leqq A$. If $f, g \in \Omega_A$ and if h is an entire function such that $fh = g$, then we must have $h \in \Omega_A$. Every principal ideal in Ω_A is determined by its local ideals, or, what is the same thing, if $P, S \in \Omega_A$ have the property that*

the cospectrum of S contains the cospectrum of P, then $S = PT$ for some $T \in \mathfrak{Q}_A$.

We have the immediate

COROLLARY. *All the results of Theorem 4 for the rings $\mathfrak{Q}_A$ hold also for the ring $\mathfrak{Q}$ of all entire functions of finite order.*

The results of Theorem 4 and its corollary extend to the following more general situation: Let ϕ be a positive, even, continuous function of one real variable, with ϕ monotonically increasing to infinity. We call ϕ an *admissible* function if

(a) $\phi(x) = O(|x|^p)$ for some p.

(b) There exists a p satisfying (a) such that, for all $r > 0$,

$$\sum_{j=0}^{\infty} 2^{-j(p+2)} \phi(2^{j+3} r) \leqq d\phi(r), \tag{2}$$

where d is a constant depending only on ϕ. A family Φ of admissible functions ϕ is called an *admissible* family if there exists an admissible funtcion ψ (not necessarily in Φ) such that, for every r and every $\phi \in \Phi$, $\phi(r) \geqq \psi(r)$. As examples of admissible functions we have the functions $\phi(r) = r^p$ for any $p > 0$. An example of an admissible family is all funtcions $\phi(r) = r^p$ for all $p > q \geqq 0$.

If ϕ is an admissible function, we denote by Q_ϕ the ring of entire functions f of n complex variables which satisfy

$$f(z) = O[\exp(\phi(\| z \|))]. \tag{3}$$

For any admissible family Φ, we define $Q_\Phi = \bigcap_{\phi \in \Phi} Q_\phi$ and, for Ψ an arbitrary family of admissible functions, we define $Q^*_\Psi = \bigcup_{\psi \in \Psi} Q$. Then we can easily generalize Theorem 4 and its corollary to

THEOREM 5. *Let Φ be an admissible family. Then for any $f, g \in Q_\Phi$, if h is an entire function satisfying $fh = g$, then we must have $h \in Q_\Phi$. Every principal ideal in Q_Φ is determined by its local ideals, that is, if $P, S \in Q_\Phi$ have the property that the cospectrum of S contains the cospectrum of P, then $S = PT$ for some $T \in Q_\Phi$. These results also hold for the spaces Q^*_Ψ for any family Ψ of admissible functions.*

Remark 1. Theorem 5 obviously contains Theorem 4 and its corollary and Theorem 6 of Section 4 as special cases.

Remark 2. Theorem 5 itself can be extended to more general families, for the condition (b) in the definition of admissible can certainly be improved and even condition (a) can be slightly ameliorated. However, a recent result of Hayman on the minimum modulus makes it extremely unlikely that condition (a) can be entirely omitted (see *Proc. Lond. Math. Soc.*, 1952, pp. 469-512).

6. The case $n = 1$. Throughout this section we shall suppose that $n = 1$. We shall give a simplification of the solution by L. Schwartz [12] of problem 2 of Section 3. It is fairly simple to prove from this (see [12]) that every ideal in $\boldsymbol{H}'$ is the ideal generated by two functions of $\boldsymbol{H}'$, and that every variety in $\mathfrak{M}$ is the variety generated by a single element. In Section 3 it was shown how this solution of Problem 2 implies that the spectrum of the union of two varieties is the spectral union of their spectra. Thus, the results of this section will conclude the solutions of all the problems of Section 3.

PROPOSITION. *Let I be an ideal in $\boldsymbol{H}'$ and $F \in I$, $F \neq 0$. Suppose that, for some $a \in C$, F has a zero of order $m > 0$ and some $G \in I$ has no zero at a. Then $F/(Z-a) \in I$.*

Proof. Let W be the annihilator variety of the inverse Fourier transform of I; denote by S the inverse Fourier transform of $F/(Z-a)$, and call V the variety generated by $\{S*f\}_{f \in W}$. From the formula $T \cdot S * f = T * S \cdot f$ for any $f \in \mathfrak{M}$, $T \in \mathfrak{M}'$, it follows immediately that T is in the annihilator ideal J of V if and only if $T * S$ is in the annihilator ideal of W.

Call K the Fourier transform of J. The above shows us that $P \in K$ if and only if $PF/(Z-a) \in I$. Assume $F/(Z-a) \notin I$; then $(Z-a) \in K$ but $1 \notin K$. Thus, V is not $\{0\}$ and, in fact, consists exactly (see Section 2) of the solutions $\alpha \exp(ia\cdot)$ for $\alpha \in C$ of the ordinary differential equation $-i(df/dZ) - af = 0$ for $f \in \mathfrak{M}$. Hence, $\exp(ia\cdot) \in W$, which implies (see Section 3) that every $Q \in I$ has a zero at a. This contradiction completes the proof.

THEOREM 1. *Every variety contains an exponential polynomial, or, what is the same thing, every ideal in $\boldsymbol{H}'$ has a zero.*

Proof. Assume I is an ideal in $\boldsymbol{H}'$ with no zero, and let $f \in I$, $f \neq 0$. We may assume f is even (for if f is not even, we may consider $ff \in I$). Let

$$f(z) = z^m \prod_{j=1}^{\infty} (1 - z^2/a_j^2)$$

be the Weierstrass-Hadamard factorization of f. For each $k > 0$, set

$$f_k(z) = \prod_{j=k}^{\infty} (1 - z^2/a_j^2).$$

Then by induction on the above proposition, we find easily that each $f_k \in I$. Moreover, it is easy to see that we can find positive numbers A, M so that, for all k and all $z \in C$,

$$|f_k(z)| \leqq \prod_{j=1}^{\infty} (1 + |z|^2/|a_j|^2) \leqq Me^{A|z|}.$$

Further, it is clear that $f_k \to 1$ in $\mathfrak{A}$. Thus, by Proposition 3 of Section 2, $f_k \to 1$ in $\boldsymbol{H}'$. Since I is closed, this means that $1 \in I$ which contradicts the fact that I is an ideal (since an ideal is $\neq \boldsymbol{H}'$).

THEOREM 2. *Every variety is determined by its spectrum. Equivalently, if I is an ideal in $\boldsymbol{H}'$ and if the cospectrum of $f \in \boldsymbol{H}'$ contains the cospectrum of I, then $f \in I$.*

Proof. Let V be a variety; call W the variety generated by the exponential polynomials of V and suppose $f \in V$, $f \notin W$. By the Hahn-Banach theorem we can find an $S \in \mathfrak{A}'$ which is zero on W but such that $S \cdot f \neq 0$. Consider the variety X generated by $\{S * g\}_{g \in V}$ ($X \neq 0$ because $S * f \neq 0$); we claim X has no exponential polynomials.

Denote by F the Fourier transform of S, and by I, J, K the respective Fourier transforms of the annihilator ideals of V, X, and W. Assume there exists an exponential polynomial in X; then there is an $a \in C$ at which every $G \in J$ vanishes. As in the proof of the above proposition, $G \in J$ if and only if $GF \in I$. Thus, the above implies that every multiple of F which is in I has a zero at a of order $>$ $m =$ order of zero of F at a. Now, by construction, the cospectrum of F contains the cospectrum of I. Thus, there is a $G \in I$ whose order k of zero at a is $\leqq m$. Then $(G/(Z-a)^k)F = G(F/(Z-a)^k) \in I$, but has a zero at a of order m. This contradiction proves that X has no exponential polynomials. This contradicts Theorem 1 and so completes the proof of Theorem 2.

7. General remarks. The methods of Section 6 apply also to other spaces (but still only for $n = 1$), for example the space $\mathcal{E}$ of Schwartz (see [14], [12], and [8]) of indefinitely differentiable functions. In that case, the proof of the proposition of Section 6 can be carried out as before. The proof of Theorem 1 of Section 6 does not seem to extend to $\mathcal{E}$; however, if I is an ideal in $\boldsymbol{E}'$ (see [8]) which has no zero, then for $f \in I$, $f \neq 0$, and f

rapidly decreasing on the real axis, it is shown by Schwartz (see [12]) that also $f' \varepsilon I$. From this it follows easily (see [12]) that $1 \varepsilon I$. This proves the analog of Theorem 1 of Section 6 for $\boldsymbol{E}$. The analog of Theorem 2 then follows as before.

There are two essential difficulties in extending the methods of Section 6 to $n > 1$. The first is the fact that the ideals in the spaces $\mathfrak{P}_a$ (see Section 5) need not be principal for $n > 1$. Thus, no analog of $F/(Z - a)$ which is used in the proof of the proposition of Section 6 can be found. But even if this difficulty could be surmounted, the following difficulty remains: For $n > 1$, there exist functions in $\mathcal{M}$ other than exponential polynomials which are solutions of constant-coefficient partial differential equations. Thus, an entirely new approach is needed for the problem. This will be done in Part II of this series.

Each $S \varepsilon \mathcal{M}'$ defines an element of the space $\boldsymbol{D}'$, or even of $\boldsymbol{E}'$ (see [8]), namely the restriction T of S to $\boldsymbol{D}$. It is clear that $\boldsymbol{D}$ is dense in $\mathcal{M}$, so that T determines S uniquely. We want to show now that the Fourier transform M of S defined in Section 2 is, essentially, the inverse Fourier transform U of T, as defined in [8]. Using the notation of [8], if $F \varepsilon \boldsymbol{D}$, and if v is a measure of compact carrier which represents S (hence also T), then by an easily justified change in the order of integration,

$$U \cdot f = T \cdot f = \int F(z)\, dv(z) = \int dv(z) \int f(x) e^{-ix \cdot z} dx$$
$$= \int f(x)\, dx \int e^{-ix \cdot z} dv(z) = \int M(-x) f(x) = \mathfrak{j}\check{M} \cdot f.$$

Thus, $U = \mathfrak{j}\check{M}$ which is the desired result.

THE JOHNS HOPKINS UNIVERSITY AND THE INSTITUTE FOR ADVANCED STUDY.

BIBLIOGRAPHY.

[1] S. Banach, *Théorie des Opérations Linéaires*, Monografje Matematyczne, Warsaw, 1932.

[2] S. Bochner and W. T. Martin, *Several Complex Variables*, Princeton, 1948.

[3] H. Cartan, "Idéaux et modules de fonctions analytiques de n variables complexes," *Bulletin de la Societe Mathematique de France*, vol. 78 (1950), pp. 28-64.

[4] ———, "Variétés analytiques complexes et cohomologie," *Colloque sur les Fonctions de Plusieurs Variables*, Bruxelles, 1953.

[5] – ——, *Faisceaux Analytiques*, Seminaire E.N.S., Paris, 1951-52, Chapt. XV-XX (mimeographed).

[6] J. Dieudonné and L. L. Schwartz, "La dualité dans les espaces ($\mathcal{F}$) et ($\mathcal{LF}$)," *Annales de l'Institut Fourier* (Grenoble), vol. I (1950), pp. 61-101.

[7] L. Ehrenpreis, *Theory of distributions for locally compact spaces*, Columbia University Thesis, 1953 (to appear).

[8] ———, "Analytic functions and the Fourier transform of distributions," *Annals of Mathematics* (to appear).

[9] ———, "Solution of some problems of Division, part I," *American Journal of Mathematics*, vol. 76 (1954), pp. 883-903.

[10] B. Malgrange, "Sur quelques propriétés des equations de convolution," *Comptes Rendus des Séances de l'Académie des Sciences*, vol. 238 (1954), pp. 2219-2221.

[11] G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, vol. II, Berlin, 1925.

[12] L. Schwartz, "Théorie générale des fonctions moyenne-périodiques," *Annals of Mathematics*, vol. 48 (1947), pp. 857-929.

[13] ———, *Etude des Sommes d'Exponentielles Réelles*, Paris, 1943.

[14] ———, *Théorie des Distributions*, vol. I-II, Paris, 1950-51.

[15] ———, "Analyse et synthèse harmonique dan les espaces de distributions," *Canadian Journal of Mathematics*, vol. 3 (1951), pp. 503-512.

[16] E. C. Titchmarsh, *The Theory of Functions*, Oxford, 1932.

[17] ———, *Theory of Fourier Integrals*, Oxford, 1937.

[18] H. Whitney, "On ideals of differentiable functions," *American Journal of Mathematics*, vol. 70 (1948), pp. 635-658.

[19] N. Wiener, *The Fourier Integral and Certain of its Applications*, Cambridge, 1933.

ON UNIFORM DINI CONDITIONS IN THE THEORY OF LINEAR PARTIAL DIFFERENTIAL EQUATIONS OF ELLIPTIC TYPE.*

By PHILIP HARTMAN and AUREL WINTNER.

---

1. Introduction. Since Hölder's thesis [8] and the subsequent work of Korn and Lichtenstein (for references, cf. [14]) dealing with existence theorems for linear elliptic partial differential equations of second order, it has become standard practice to assume a uniform Hölder degree of continuity for the data. That is, it is assumed that the given functions (or suitable derivatives of them) satisfy a condition of the form

$$|f(P)-f(Q)| \leqq \text{const.}\,|PQ|^{\lambda}, \qquad 0<\lambda<1. \tag{1}$$

The proof of the existence theorems then depends on obtaining an a priori estimate for the degree of continuity of the second order derivatives of the solutions of the given, or of a related, partial differential equation. This a priori estimate is also of the form (1) (cf. [10], pp. 25-32); it allows the definition, and the proof for the convergence, of a sequence of successive approximations (cf. [11]).

It will be shown in the present paper that, in some of the existence theorems, the uniform Hölder degree of continuity for the data can be replaced by assumptions of a uniform degree of continuity,

$$|f(P)-f(Q)| \leqq \text{const.}\,\alpha(|PQ|), \tag{2}$$

where $\alpha=\alpha(r)$ is a monotone function satisfying Dini's condition (cf. [4], p. 102 and [5], pp. 210-219), that is,

$$\int_{+0} r^{-1}\alpha(r)\,dr<\infty, \qquad d\alpha(r)\geqq 0. \tag{3}$$

The proof of the resulting existence theorems will not depend on successive approximations. They will depend on an a priori estimate of the degree of continuity of the form

$$|f(P)-f(Q)| \leqq K\cdot\text{Const.}\,\beta(|PQ|) \tag{4}$$

for the second order partial derivatives of solutions. In (4), $\beta=\beta(r)$ is a function determined by $\alpha(r)$ and satisfying

$$\beta(r)\to 0 \text{ as } r\to 0, \tag{5}$$

---

* Received December 27, 1954.

Const. is a function of const. in (2), and K is a constant depending on the diameter of the domain under consideration. (In the case (1), $\alpha(r) = \beta(r) = r^\lambda$, and K is a Korn constant.) The fact that $\beta(r)$ need not satisfy a Dini condition means that a sequence of successive approximations cannot in general be formed; cf. the example in Section 13 below. The existence proof can, however, be completed by using the method of equicontinuous functions.

Dini's results [5], involving a condition of the type (2), (3) in the theory of elliptic partial differential equations, antedates the work of Korn and Lichtenstein. But Dini only considers the simple equation $u_{xx} + u_{yy} + D_1 u_x + D_2 u_y + Du = E$. Dini's conditions are not expressed in the form (2), (3); instead of this, he merely requires that, uniformly in P,

$$(2') \qquad \infty > \int_{|PQ|<r} |f(P) - f(Q)| \cdot |P - Q|^{-n} \, dQ \to 0 \text{ as } r \to 0,$$

where $n = 2$ is the number of independent variables and dQ is the n-dimensional element of volume (area). This milder condition (2') can replace (2), (3) below if it is assumed, in addition, that, uniformly in P,

$$(3') \qquad |f(P) - f(Q)| \log |PQ| \to 0 \text{ as } Q \to P.$$

(For conditions, sharper than (2'), for the existence, but not for the continuity, of the second derivatives of a logarithmic potential, cf. [15].)

2. Statement of the results. In this paper, the method described in connection with (2)-(5), a method which has other applications also, will be used to give a detailed proof of the following theorem:

(*) *Let $(g_{ik}) = (g_{ik}(x, y))$ be a 2 by 2, positive definite, symmetric matrix defined in a vicinity of $(x, y) = (0, 0)$ in such a way that the matrix elements $f = g_{11}, g_{12} = g_{21}, g_{22}$ satisfy (2), where $\alpha = \alpha(r)$ is a continuous monotone function satisfying (3). Then, in a vicinity of $(x, y) = (0, 0)$, there exist mappings $u = u(x, y)$, $v = v(x, y)$ of class C^1 satisfying*

$$(6) \qquad \partial(u, v)/\partial(x, y) \neq 0$$

and transforming the Riemann metric

$$(7) \qquad ds^2 = g_{11} dx^2 + 2 g_{12} dx dy + g_{22} dy^2$$

into the conformal normal form

$$(8) \qquad ds^2 = \tau(du^2 + dv^2), \qquad \tau = \tau(u, v) > 0.$$

In addition, the first order partial derivatives of u and v will satisfy a condition of the type (4)-(5), where $\beta(r)$ is determined by $\alpha(r)$, the Const. in (4) is a function of the const. in (2) and of the bounds for g_{ik}, $(g_{11}g_{22}-g_{12}^2)^{-1}$ and g_{11}^{-1}, finally K is a constant (depending on $\alpha(r)$ and the diameter of the (x,y)-neighborhoods involved).

When $\alpha(r)=r^\lambda$, the assertion (*) reduces to a result of Lichtenstein ([13]; for another proof, cf. [2]). It is known ([7]; cf. [3], Appendix) that (*) is false if it is only assumed that the g_{ik} are continuous.

The partial differential equations connected with the problem of transforming (7) into (8) are of the form

$$v_x=-B_2u_x-Cu_y, \qquad v_y=Au_x+B_1u_y, \tag{9}$$

where

$$A=g_{22}/g, \quad B_1=B_2=-g_{12}/g, \quad C=g_{11}/g, \quad g=(\det g_{ik})^{\frac{1}{2}}. \tag{10}$$

Following the procedure of Lichtenstein [13] to obtain a solution u, v of (9), it will be shown that if R is sufficiently small, then the first boundary value problem of

$$(Au_x+B_1u_y)_x+(B_2u_x+Cu_y)_y=0 \tag{11}$$

on $x^2+y^2\leqq R^2$ has a C^1-solution, provided that the assigned boundary function is sufficiently smooth. By a C^1-solution $u=u(x,y)$ of (11) is meant a function of class C^1 on $x^2+y^2\leqq R^2$ which satisfies

$$\int_J (B_2u_x+Cu_y)\,dx-(Au_x+B_1u_y)\,dy=0 \tag{12}$$

for every piecewise smooth Jordan curve J in $x^2+y^2\leqq R$ (and which reduces to the given boundary values on $x^2+y^2=R^2$).

In the considerations below, it will not be assumed that $B_1=B_2$, as in (10), but only that the functions

$$a=A, \quad b=\tfrac{1}{2}(B_1+B_2), \quad c=C \tag{13}$$

satisfy

$$ac-b^2>0 \quad \text{and} \quad a>0. \tag{14}$$

In other words, it will be assumed that (9) is elliptic but not that it is self-adjoint; cf. [1]. It will be clear from the proof that the method can be applied to the inhomogeneous equation

$$(Au_x+B_1u_y)_x+(B_2u_x+Cu_y)_y+Du=E, \tag{15}$$

which in an integrated form is equivalent to

$$(16) \qquad \int_J (B_2 u_x + C u_y)\,dx - (A u_x + B_1 u_y)\,dy = \iint_T (Du - E)\,dx dy,$$

where T is the interior of the arbitrary piecewise smooth Jordan curve J.

(**) *Let* $f = A(x,y)$, $B_1(x,y)$, $B_2(x,y)$, $C(x,y)$ *be functions on* $x^2 + y^2 \leqq R^2$ *satisfying* (2)-(3), *let* $D(x,y)$, $E(x,y)$ *be continuous, and let* $\phi(x,y)$ *be of class* C^2 *there. Then there exists a number* R_0 (> 0), *depending on* const. *in* (2) *and on the bounds of* $|A|$, $|B_1|$, $|B_2|$, $|C|$, $|D|$, *with the property that if* $R \leqq R_0$, *then* (15) (*that is,* (16)) *has a* C^1*-solution* $u = u(x,y)$ *on* $x^2 + y^2 \leqq R^2$ *satisfying the boundary condition* $u = \phi$ *on* $x^2 + y^2 = R^2$.

(*This solution is of class* C^2 *if* A, B_1, B_2, C *are of class* C^1 *and their partial derivatives satisfy conditions of the type* (2)-(3) *and if* D, E *and the second order partial derivatives of* ϕ *satisfy conditions of the type* (2)-(3).)

The main interest in this theorem lies, of course, in the existence of non-constant solutions for (15), rather than in the solvability of a boundary value problem. For references to known results which depend on (1), rather than (2)-(3), cf. [14], pp. 1294-1927. The last (parenthetical) part of (**) will be seen (Section 14) to be a consequence of a modification of the proof of the first part; the conditions (2)-(3) on D, E and on the derivatives of A, B_1, B_2, C and ϕ can be relaxed to a uniform Dini condition (2′), where $n = 2$.

The assertions concerning (11) and (15) can be extended to the case of elliptic partial differential equations of second order in more than two independent variables. In this case, the definition of a C^1-solution of the analogue of (11) or (15) is not given by (12) or (16) but by an integro-differential equation involving Green's functions; cf. Section 7 below.

The proof for the existence of C^1-solutions of (11) will depend on variants of Korn's procedures [10] (adapted to (2), instead of (1)), as modified by E. Hopf [9]. While *loc. cit* [9], pp. 202-206, integrals depending only on the logarithmic singularity of the Green functions are dealt with, below it will be necessary to deal with the Green functions themselves, in order to obtain estimates which are valid inside (and on) the boundary curve of the domain.

Although the ideas underlying the proof of (*), as indicated in Section 1, are quite simple, the details will be involved. The arrangement of the proof of (*) will be as follows:

In Section 3, the main result (Lemma 1), dealing with a priori estimates

for the degree of continuity of the partial derivatives of C^1-solutions of (11), will be stated, but not proved. Assuming Lemma 1, the existence theorem (Lemma 2) for the first boundary value problem belonging to (11) will be stated and proved in Section 4. A proof of (*) will then be deduced from this result in Section 5.

The proof of the main Lemma 1 will be given in Sections 6-12. In Section 6, the sheaf of Green functions will be introduced and their desired properties will be stated, but not proved, in Lemma 3. In Section 6, there will also be stated the analogues (Lemmas 4 and 5) of Hopf's variants of Korn's results. In Section 7, following Lichtenstein ([13], Section 2), the differential equation (11) will be transformed into an integro-differential equation involving the Green functions. Assuming Lemmas 3, 4, 5 of Section 6, the main Lemma 1 will be proved in Section 8. Finally, Lemma 3 will be proved in Sections 9-11 and Lemmas 4, 5 in Section 12.

Section 13 will contain an example mentioned in Section 1 in connection with successive approximations and (2)-(3).

3. A priori estimates. Let $a = a(r)$, where $0 \leqq r < \infty$, be a continuous monotone function satisfying (3). In terms of $a(r)$ and a given $R > 0$, define $\beta(r) = \beta(r; R)$ as follows:

$$\beta(r) = (r + a(r)) \log (8R/r) + \int_0^{4r} r^{-1} a(r)\,dr + r \int_r^{2R} r^{-2} a(r)\,dr \tag{17}$$

for $0 < r \leqq 2R$ (the choice of the factor 8 in $\log 8R/r$ assures that $\log 8R/r \geqq 1$ for $0 < r \leqq 2R$). By virtue of (3),

$$\beta(r) \to 0 \text{ as } r \to 0. \tag{18}$$

Let $f = A(x, y)$, $B_1(x, y)$, $B_2(x, y)$, $C(x, y)$ be real-valued functions defined on C + D, where

$$\text{C: } x^2 + y^2 = R^2 \quad \text{and} \quad \text{D: } x^2 + y^2 < R^2, \tag{19}$$

and let these four functions satisfy

$$|f(P) - f(Q)| \leqq k_1 a(|PQ|). \tag{20}$$

Let the constant k_1 be chosen so large that

$$|f(P)| \leqq k_1. \tag{21}$$

If $a = a(x, y)$, $b(x, y)$, $c(x, y)$ are defined by (13), suppose that (14) holds. Let k_1 be so large that

$$d^2 = ac - b^2 \geqq 1/k_1 \ (> 0), \qquad a \geqq 1/k_1 \ (> 0). \tag{22}$$

Let $\phi = \phi(x, y)$ be a (real-valued) function of class C^2 on $C + D$. Let the constant k_2 be chosen so that if f denotes ϕ or any of its first and second order partial derivatives, then

$$|f(P)| \leqq k_2. \tag{23}$$

The main lemma will be the following assertion, supplying an a priori estimate for the degree of continuity of first order derivatives of C^1-solutions of (11):

LEMMA 1. *There exists a pair of functions of k_1, say $R_0(k_1)$ and $c_1(k_1)$, with the property that if $R \leqq R_0$ and if $u = u(x, y)$ is a C^1-solution of* (11) *on* $C + D$ *satisfying the boundary condition*

$$u = \phi \text{ on } C, \tag{24}$$

then the first order partial derivatives $f = u_x, u_y$ are subject to the estimates

$$|f| \leqq c_1(k_1)k_2, \tag{25$_1$}$$

$$|f(P) - f(Q)| \leqq c_1(k_1)k_2\beta(|PQ|) \tag{25$_2$}$$

on $C + D$, *where $\beta(r) = \beta(r; R)$ is given by* (17).

Remark 1. Note that $c_1(k_1)$ does not depend on R $(\leqq R_0)$.

Remark 2. It will be clear from the proof that conditions (2)-(3) on $f = A, B_1, B_2, C$ can be relaxed to (2′), (3′) in the following sense: Let $E = E(r, P)$ denote the set of points Q in $x^2 + y^2 \leqq R^2$ satisfying $|Q - P| \leqq r$. Assume that

$$\epsilon_1(r) = \text{l. u. b.} \iint_E |f(P) - f(Q)| \cdot |P - Q|^{-2}\, dQ \qquad (dQ = dxdy)$$

exists, where the l. u. b. refers to P in $x^2 + y^2 \leqq R^2$ and $f = A, B_1, B_2$ and C, and satisfies $\epsilon_1(r) \to 0$ as $r \to 0$. Then

$$\epsilon_2(r) = \text{l. u. b.}\, r \iint_{D-E} |f(P) - f(Q)| \cdot |P - Q|^{-3}\, dQ$$

(exists and) satisfies $\epsilon_2(r) \to 0$ as $r \to 0$. Assume that

$$\epsilon_3(r) = \text{l. u. b.}\, (\log |PQ|^{-1})\, |f(P) - f(Q)|,$$

(exists and) satisfies $\epsilon_2(r) \to 0$ as $r \to 0$, where l. u. b. refers to P in $x^2 + y^2 \leqq R^2$, Q in $E(r, P)$ and $f = A, B_1, B_2, C$. Then Lemma 1 remains true if (17) is replaced by

$$\beta(r) = r \log (8R/r) + \epsilon_1(r) + \epsilon_2(r) + \epsilon_3(r).$$

Remark 3. It does not follow from the statement of Lemma 1 that if $a(r) = r^\lambda$, where $0 < \lambda < 1$, then $\beta(r)$ can be chosen to $\beta(r) = r^\lambda$ (Korn). That this is so follows, however, from the fact that if (17) satisfies a Dini condition,

$$\int_{+0} r^{-1}\beta(r)\,dr < \infty,$$

then Lemma 1 can be improved by omitting the term $a(r)\log 1/r$ in (17). The proof of this fact is similar to the application (p. 209) of the *Korollar* (p. 204) in [9].

It will be clear from the considerations to follow that it is sufficient to prove Lemma 1 for the case that A, B_1, B_2, C and ϕ are smooth; so that u is of class C^2.

4. Existence theorem for (11). The existence theorem, mentioned for (11) above, is the following Lemma 2. The assumptions on A, B_1, B_2, C and ϕ are those mentioned in connection with (19)-(22) and (23), respectively.

LEMMA 2. *If $R \leqq R_0$, there exists one and only one C^1-solution $u = u(x, y)$ of* (11) *on* C + D *satisfying the boundary condition* (24).

The existence assertion in this lemma will be deduced from the fact that Lemma 2 is known if A, B_1, B_2, C and ϕ are smooth (say, analytic); cf. [13], Sections 2-4 (where it is assumed that $B_1 \equiv B_2$, but this assumption is not actually used).

There exist sequences $\{A_n\}$, $\{B_{1n}\}$, $\{B_{2n}\}$, $\{C_n\}$ of analytic functions on C + D satisfying, as $n \to \infty$,

$$(26_1) \qquad A_n \to A, \quad B_{1n} \to B_1, \quad B_{2n} \to B, \quad C_n \to C$$

uniformly on C + D and such that the inequalities (19)-(22), where k_1 is independent of n, are satisfied (the existence of such approximating sequences follows, for instance, from the theory of Fourier series). Similarly, there exists a sequence $\{\phi_n\}$ of smooth functions in C + D satisfying, as $n \to \infty$,

$$(26_2) \qquad \phi_n \to \phi$$

uniformly on C + D and such that ϕ_n and its first and second order partial derivatives satisfy (23), where k_2 is independent of n.

Let (11_n) denote the partial differential equation (11) in which A, B_1, B_2, C are respectively replaced by A_n, B_{1n}, B_{2n}, C_n and let (12_n) denote the integral relation corresponding to (12). Finally, let (24_n) denote the

boundary condition in which ϕ is replaced by ϕ_n. If $u = u_n(x, y)$ denotes the solution of the boundary value problem (11_n), (24_n) and if $R \leqq R_0$, it follows from Lemma 1 and from (26_2) that the sequences $\{u_n\}$, $\{u_{nx}\}$, $\{u_{ny}\}$ are uniformly bounded and equicontinuous on C + D.

Consequently, after a selection and a renumbering of a subsequence, it can be supposed that, as $n \to \infty$,

$$u = \lim u_n, \qquad u_x = \lim u_{nx}, \qquad u_y = \lim u_{ny} \tag{27}$$

exist uniformly on C + D. It follows from (26_2) and (24_n) that (24) holds. From (26_1), (27) and a term-by-term integration of (12_n), as $n \to \infty$, it is seen that (12) holds for every piecewise smooth Jordan curve J in D + C. This completes the existence proof.

The proof of uniqueness follows standard procedures for the proof of the weak maximum principle. The identity (12) in J implies the Green relation

$$\int_J u\{(B_2 u_x + C u_y)dx - (A u_x + B_1 u_y)dy\} = -\iint_T (a u_x^2 + 2b u_x u_y + c u_y^2)dxdy,$$

where the double integral is over the interior T of J; cf. [6], Lemma, p. 761. Choose J = C and suppose that $u = 0$ on C. Then

$$\iint_D (a u_x^2 + 2b u_x u_y + c u_y^2)dxdy = 0;$$

so that, by (14), $u_x \equiv u_y \equiv 0$ on C + D, hence $u \equiv 0$. Thus (11) has exactly one C^1-solution satisfying the boundary condition $u = 0$ on C. In view of the linearity of (11), this completes the proof of the uniqueness in Lemma 2.

5. Proof of (*). Assertion (*) can now be proved by arguments of Lichtenstein [13], Section 5; its proof will be given only for the sake of completeness.

In terms of the g_{ik}, define A, $B_1 = B_2$, C by (10). Then, by assumption, $f = A_1$, $B_1 = B_2$, C satisfy (20)-(22) on C + D for suitable choices of R and k_1. Thus, if R is sufficiently small and ϕ is suitably chosen, the boundary value problem (11), (24) has a (unique) C^1-solution $u = u(x, y)$. It follows from the integrated form (12) of (11) that there exists a function $v = v(x, y)$ (unique up to an additive constant) which is of class C^1 on C + D and satisfies the system (9).

Hence, all that remains to be shown is that u and v satisfy (6) if R is

sufficiently small and $\phi(x, y)$ is suitably chosen. To this end, choose a $k_2 > 0$, and let $\phi(x, y)$ be a function of class C^2 on C + D such that ϕ and its first and second order partial derivatives satisfy (23) and, in addition, the tangential derivative of ϕ at some point of C is not 0. For example, let the point (x, y) be $(0, R)$ and let $|\phi_x(0, R)| = k_2 \neq 0$. Since (24) implies that the tangential derivatives of u and ϕ coincide on C, it follows that $|u_x(0, R)| = k_2 \neq 0$. Since $c_1(k_1)$ in (25_2) does not depend on $R\ (\leqq R_0)$, it follows from the definition of $\beta(r) = \beta(r; R)$ that $u_x(x, y) \neq 0$ in C + D if R is sufficiently small.

The inequality $u_x(x, y) \neq 0$ on C + D implies (6), in view of (9) and (14). This proves (*).

6. Green's functions. In what follows, real- or complex-valued functions $f(x, y)$ of (x, y) will be denoted by $f(z)$. Correspondingly, $f_s(z)$, where $s = x$ or $s = y$, denotes $\partial f(x, y)/\partial s$.

Let a, b, c, d be real constants satisfying (14). Let $\zeta = \xi + i\eta$, $z = x + iy$ and let $G(\zeta, z) = G(\zeta, z; a, b, c)$ be the Green function of

$$aw_{xx} + 2bw_{xy} + cw_{yy} = 0 \tag{28}$$

on the circle D belonging to the boundary condition

$$w = 0 \text{ on C.} \tag{29}$$

Thus, if $h = h(x, y)$ is a sufficiently smooth function on C + D, then

$$w(x, y) = \tfrac{1}{2\pi} \iint_{\mathrm{D}} h(\zeta)\, G(\zeta, z)\, d\xi d\eta \tag{30}$$

is the solution of

$$aw_{xx} + 2bw_{xy} + cw_{yy} = h \tag{31}$$

in D which vanishes on C.

The proof of Lemma 1 will be made to depend on some properties of the sheaf of Green functions $G(\zeta, z; a, b, c)$, where the constants (a, b, c) are subject to the inequalities

$$1/k_1 \leqq a, c \leqq k_1, \qquad d^2 = ac - b^2 \geqq 1/k_1, \tag{32}$$

in which k_1 is a positive constant.

For the purpose of denoting partial derivatives of G in Lemma 3, let $\sigma = \xi$ or $\sigma = \eta$, and $s, t = x$ or y, finally $e = a$, b or c.

LEMMA 3. *There exists a constant $c_2 = c_2(k_1)$, independent of R, such that*

$$|G_s| \leqq c_2/|\zeta - z|, \qquad |G_{\bar{s}}| \leqq c_2/|\zeta - z|, \tag{33}$$

$$|G_{\sigma s}| \leqq c_2/|\zeta - z|^2, \qquad |G_{\sigma \bar{s}}| \leqq c_2/|\zeta - z|^2, \tag{34}$$

$$|G_{\sigma s t}| \leqq c_2/|\zeta - z|^3, \tag{35}$$

for $|\zeta| < R$, $|z| < R$, $\zeta \neq z$.

Lemma 3 will be proved in Sections 9-11 below.

The following two lemmas are analogous to E. Hopf's variants ([9], pp. 202-206) of Korn's results ([10], pp. 25-32).

LEMMA 4. *Let $H(\zeta, z; z_0)$ be defined for $\zeta\ (\neq z)$, z, z_0 subject to $|\zeta| < R$, $|z| < R$, $|z_0| < R$, let H possess there continuous partial derivatives with respect to x and y, and let it satisfy, for some constant k_3,*

$$|H| \leqq k_3/|\zeta - z|, \quad |H(\zeta, z; z_0) - H(\zeta, z; z^0)| \leqq k_3 a(|z_0 - z^0|)/|\zeta - z|, \tag{36}$$

$$|H_s| \leqq k_3/|\zeta - z|^2 \text{ for } s = x \text{ and } s = y. \tag{37}$$

Then, if $h(x, y)$ is a continuous function on $C + D$ and k_4 is a constant satisfying

$$|h| \leqq k_4, \tag{38}$$

the function

$$\nu(z_0) = \iint_D h(\zeta) H(\zeta, z_0; z_0)\, d\xi d\eta \tag{39}$$

satisfies

$$|\nu(z_0) - \nu(z^0)| \leqq K k_3 k_4 \beta^1(|z_0 - z^0|), \tag{40}$$

where K is an absolute constant and

$$\beta^1(r) = \beta^1(r; R) = Ra(r) + r \log(8R/r). \tag{41}$$

LEMMA 5. *Let $L(\zeta, z; z_0)$ be defined for $\zeta\ (\neq z)$, z, z_0 subject to $|\zeta| < R$, $|z| < R$, $|z_0| < R$, let L possess continuous partial derivatives with respect to x and y there and let it satisfy, for some constant k_5,*

$$|L| \leqq k_5/|\zeta - z|^2, \quad |L(\zeta, z; z_0) - L(\zeta, z; z^0)| \leqq k_5 a(|z_0 - z^0|)/|\zeta - z|^2, \tag{42}$$

$$|L_s| \leqq k_5/|\zeta - z|^3 \text{ for } s = x \text{ and } s = y. \tag{43}$$

Let $h = h(x, y)$ be continuous on $C + D$ and let k_4 satisfy (38). *Let $l = l(x, y)$ be defined on $C + D$ and satisfy*

$$|l(z_1) - l(z_2)| \leqq k_6 a(|z_1 - z_2|). \tag{44}$$

Then the function

$$\mu(z_0) = \iint_D (l(\zeta) - l(z_0))h(\zeta)L(\zeta, z_0; z_0)\,d\xi d\eta \tag{45}$$

satisfies

$$|\mu(z_1) - \mu(z_2)| \leqq Kk_4k_5k_6\beta^2(|z_1 - z_2|), \tag{46}$$

where K is an absolute constant and $\beta^2(r) = \beta^2(r; R)$ is defined by

$$a(r)\{\int_0^{2r} r^{-1}a(r)\,dr + \log(2R/r)\} + \int_0^{4r} r^{-1}a(r)\,dr + r\int_r^{2R} r^{-2}a(r)\,dr.$$

The proof of Lemma 4 is similar to, but simpler than, the proof of Lemma 5 and will therefore be omitted, Lemma 5 will be proved in Section 12 below.

Granting Lemmas 3, 4 and 5, the proof of Lemma 1 will be given in the next two sections.

7. The integro-differential equation. In this section and the next, it is assumed that A, B_1, B_2, C and ϕ are smooth (say, analytic). Let $u = u(x, y)$ be a solution of the boundary value problem (11), (24). Put

$$w = u - \phi, \tag{47}$$

so that (24) gives

$$w = 0 \text{ on } C \tag{48}$$

and (11) becomes

$$(A(w+\phi)_x + B_1(w+\phi)_y)_x + (B_2(w+\phi)_x + C(w+\phi)_y)_y = 0. \tag{49}$$

Let $z_0 = x_0 + iy_0$ be a point of D. The differential equation (49) for w can be written as

$$a_0w_{xx} + 2b_0w_{xy} + c_0w_{yy} = h, \tag{50}$$

where

$$\begin{aligned} h &= h_1 - h_{2x} - h_{3y}, \quad h_1 = -a_0\phi_{xx} - 2b_0\phi_{xy} - c_0\phi_{yy}, \\ h_2 &= (A - A_0)(w+\phi)_x + (B_1 - B_{10})(w+\phi)_y, \\ h_3 &= (B_2 - B_{20})(w+\phi)_x + (C - C_0)(w+\phi)_y; \end{aligned} \tag{51}$$

(the superscript 0 denotes that the argument of the function is $z_0 = x_0 + iy_0$). In view of (48) and (50),

$$2\pi w(z) = \iint_D h(\zeta)G(\zeta, z; a_0, b_0, c_0)\,d\xi d\eta. \tag{52}$$

Since G vanishes on the boundary of D, partial integrations of the terms involving h_{2x}, h_{3y} transform the last formula into

$$2\pi w(z) = \iint_D (h_1 G + h_2 G_\xi + h_3 G_\eta)\, d\xi d\eta \tag{52'}$$

(the fact that the singularity of G at $\zeta = z$ is of logarithmic order assures that this partial integration is permissible).

Since h_2, h_3 vanish at $z = z_0$ and $f = A, B_1, B_2, C$ satisfy (20), the Dini condition (3) and standard procedures in potential theory show that, if $s = x$ or $s = y$,

$$2\pi w_s(z_0) = \iint_D (h_1 G_s + h_2 G_{\xi s} + h_3 G_{\eta s})\, d\xi d\eta, \tag{53}$$

where the argument of h_1, h_2, h_3 is ζ and that of the partial derivatives of G is $(\zeta, z_0; a_0, b_0, c_0)$.

8. Proof of Lemma 1. For a bounded function f on D, let

$$\| f \| = \text{l. u. b.} \, | f | \text{ on D.} \tag{54}$$

The symbol c_1 will denote a constant depending on k_1 and independent of R ($\leqq R_0$), c_2 a constant depending only on k_1, and K an absolute constant

From the definition of h_1 and from (21), (23) and (33),

$$\left| \iint_D h_1 G_s d\xi d\eta \right| \leqq c_2 k_1 k_2 2\pi R.$$

From the definition of h_2 and from (21), (23) and (34),

$$\left| \iint_D h_2 G_{\xi s} d\xi d\eta \right| \leqq c_2 k_1 (\| w_x \| + \| w_y \| + 2k_2)(2\pi) \int_0^{2R} r^{-1} a(r)\, dr.$$

A similar estimate holds for the third term on the right of (53). Hence $\| w_x \| + \| w_y \|$ does not exceed

$$2c_2 k_1 k_2 (R + 4 \int_0^R r^{-1} a(r)\, dr) + 2c_2 k_1 (\| w_x \| + \| w_y \|) \int_0^{2R} r^{-1} a(r)\, dr.$$

Thus, if R is so small that

$$2c_2 k_1 \int_0^{2R} r^{-1} a(r)\, dr \leqq \tfrac{1}{2}, \qquad c_2 = c_2(k_1), \tag{55}$$

it follows that

$$\| w_x \| + \| w_y \| \leqq 4c_2k_1k_2\Big(R + 4\int_0^R r^{-1}a(r)\,dr\Big). \tag{56}$$

If $R = R_0(k_1)$ is a fixed positive number satisfying (55), then the assertion of Lemma 1 concerning (25_1) follows from (47) and (56).

Lemma 4 is applicable to the first term on the right of (53), that is, to

$$v(z_0) = \iint_D h_1(\zeta)\, G_s(\zeta, z_0; a_0, b_0, c_0)\,d\xi d\eta, \tag{57}$$

if G_s, h_1 are identified with H, h, respectively. In fact, the first inequality of (36) is a consequence of the first in (33), with $k_3 = c_2$; the second in (36) follows, with $k_3 = 3c_2k_1$, from the second in (33), and from (13) and (20). The second line in (51) shows that k_4 in (38) can be replaced by $2k_1k_2$. Thus the assertion of Lemma 4 implies that

$$|\, v(z_0) - v(z^0)\,| \leqq Kc_1k_2\beta^1(|\, z_0 - z^0\,|) \leqq Kc_1k_2\beta(|\, z_0 - z^0\,|). \tag{58}$$

If h_2, h_3 in (53) are replaced by their equivalent expressions given by (51), the last two terms of (53) become four terms, to each of which Lemma 5 is applicable. For the sake of definiteness, one of the four terms, say the term

$$\mu(z_0) = \iint_D (A - A_0)\,(w + \phi)_x G_{\xi s}(\zeta, z_0; a_0, b_0, c_0)\,d\xi d\eta, \tag{59}$$

will be considered. If L in Lemma 5 is identified with $G_{\xi s}$, it follows from (20), (34) and (35) that (42), (43) hold, with k_5 a constant (depending only on k_1). Let l be identified with A, so that (44) holds with $k_6 = k_1$. Finally, let h in (45) be identified with $(w + \phi)_x$ in (59), so that (38) holds with $k_4 = k_2 + \| w_x \|$. Thus Lemma 5 implies that

$$|\, \mu(z_0) - \mu(z^0)\,| \leqq Kc_1(k_2 + \| w_x \|)\beta(|\, z_0 - z^0\,|),$$

where $c_1 = c_1(k_1) = c_1(k_1, R_0)$ and $\beta^2(r) \leqq c_1\beta(r)$ for a suitable choice of $c_1 = c_1(k_1)$. It follows from (56) that this can be written as

$$|\, \mu(z_0) - \mu(z^0)\,| \leqq Kc_1k_2\Big(R + 4\int_0^R r^{-1}a(r)\,dr\Big)\beta(|\, z_0 - z^0\,|).$$

Since the other terms resulting from (53) can be treated similarly, it is seen that

$$|\, w_s(z_0) - w_s(z^0)\,| \leqq c_1k_2\beta(|\, z_0 - z^0\,|), \tag{60}$$

if $c_1 = c_1(k_1) = c_1(k_1, R_0)$ and $R \leqq R_0$. The inequality (23), when applied to the case in which f is a second order partial derivative of ϕ, shows that

$$|\phi_s(z_0) - \phi_s(z^0)| \leqq k_2 |z_0 - z^0|.$$

Since $\beta(r) \geqq r$ when $r \leqq 2R$, the assertion of Lemma 1 concerning (25_2) follows from (47) and (60).

This completes the proof of Lemma 1.

9. The inequalities (33_j), (34_j), (35_j), $j = 1, 2$. Lemma 3, that is, the properties (33)-(35) of G, will be deduced from properties of the Green function

$$\gamma(\mathbf{Z}, Z) = \log |(R^2 - \bar{Z}\mathbf{Z})/R(Z - \mathbf{Z})| \tag{61}$$

belonging, in $|Z| < R$, to Laplace's equation and the boundary condition $u = 0$ on $|Z| = R$.

The change of independent variables

$$U = x/a^{\frac{1}{2}}, \qquad V = (-bx + ay)/(a^{\frac{1}{2}}d) \tag{62}$$

transforms (28) into

$$w_{UU} + w_{VV} = h, \tag{63}$$

C into an ellipse C_0 and D into the interior D_0 of C_0. Let $g(\Omega, W)$ be the Green function belonging to (63) on D_0. Then

$$G(\zeta, z) = d^{-1} g(W(\zeta), W(z)), \text{ where } W = U + iV, \tag{64}$$

$W = W(z)$ is the affine transformation (62), and $d^{-1} = \partial(U, V)/\partial(x, y)$. Thus if $Z = Z(W) = Z(W; a, b, c)$ is a conformal mapping of D_0 onto the circle $|W| < R$, it follows that

$$g(\Omega, W) = \gamma(Z(\Omega), Z(W)). \tag{65}$$

The formulae (64), (65) give G explicitly in terms of (61) and a mapping function $Z = Z(W)$. The latter is expressible in terms of elliptic functions (cf. [16]) and can be chosen so as to be analytic in the real parameters a, b, c, as well as in W. In view of (64) and (65), a formula for G is

$$G(\zeta, z; a, b, c) = d^{-1}\gamma(\mathbf{Z}, Z), \tag{66}$$

where

$$Z = Z(W(z)), \qquad \mathbf{Z} = Z(W(\zeta)), \tag{67}$$

and γ is defined by (61).

The following notation is used below for the variables which occur:

$$z = x + iy, \quad W = U + iV, \quad Z = X + iY, \quad \zeta = \xi + i\eta, \quad \mathbf{Z} = \Xi + i\mathrm{H}.$$

The symbol c_2 will denote a positive constant, not always the same, depending only on k_1 and independent of R. The letter K will signify some positive (absolute) constant.

In order to follow the dependence of G on R, let $Z = Z^1(W)$ be the function $Z(W)$ for the case $R = 1$. Then $Z(W)$, belonging to R, is $Z(W) = RZ^1(W/R)$. Note that the affine transformation (62) does not depend on R and is linear and homogeneous, so that $W(z)/R = W(z/R)$. It follows that

$$(68_1)\ c_2^{-1} \leqq |Z_W| \leqq c_2; \quad (68_2)\ |Z_{WW}| \leqq c_2/R; \quad (68_3)\ |Z_{WWW}| \leqq c_2/R^2.$$

If $e = a$, b or c and $Z = Z(W, a, b, c)$, then

$$(69_1)\ |Z_e| \leqq c_2 R; \qquad (69_2)\ |Z_{We}| \leqq c_2; \qquad (69_3)\ |Z_{WWe}| \leqq c_2/R.$$

In particular, the ratio $|Z(W_1) - Z(W_2)|/|W_1 - W_2|$ is bounded from above and from below by c_2, c_2^{-1}, respectively. Hence (62) and (22) imply that

$$(70_1) \qquad c_2^{-1} \leqq |Z(W(z)) - Z(W(\zeta))|/|z - \zeta| \leqq c_2,$$

$$(70_2) \qquad |Z_e(W(z)) - Z_e(W(\zeta))| \leqq c_2 |z - \zeta|.$$

The inequalities (69) and (70_2), involving partial derivatives with respect $e = a$, b or c, were derived by considering $Z = Z(W, a, b, c)$ as a function of W and a, b, c. The function $Z(W(z)) = Z(W(z; a, b, c), a, b, c)$, where $W = W(z; a, b, c)$ is the affine transformation (62), depends however on a, b, c in a (slightly) more complicated fashion. The derivative of $Z(W(z))$ with respect to $e = a$, b or c is $Z_W W_e + Z_e$. Since W_e depends linearly on x and y, it follows that $|W_e| \leqq c_2 R$ and $|W_e(z) - W_e(\zeta)| \leqq c_2 |z - \zeta|$. Hence (69_1) and (70_2) hold if Z_e is also an abbreviation for $Z_W W_e + Z_e$. It is in this sense that Z_e will be used below. Similar remarks hold for (69_2) and (69_3).

Let the function (61) be written as $\gamma = \gamma_1 + \gamma_2 - \log R$, where

$$(71_1) \qquad \gamma_1 = -\log |\mathbf{Z} - Z|, \qquad (71_2) \qquad \gamma_2 = \log |R^2 - \bar{Z}\mathbf{Z}|.$$

Let the equations (66)-(67), where $\gamma = \gamma_1$ or $\gamma = \gamma_2$, define G_1 and G_2; so that $G = d^{-1}(G_1 + G_2 - \log R)$. The proofs of (33)-(35) will be given separately for G_1, G_2. The inequalities analogous to (33), (34), (35) for G_j will be referred to as (33_j), (34_j), (35_j), where $j = 1, 2$.

10. Proof of (33_1), (34_1), (35_1). If $s=x$ or $s=y$, then (66)-(67) give

$$G_{js}=\gamma_{jX}X_s+\gamma_{jY}Y_s, \tag{72}$$

where, for $j=1$,

$$\gamma_{1X}=(\Xi-X)/|\mathbf{Z}-Z|^2, \qquad \gamma_{1Y}=(\mathrm{H}-Y)/|\mathbf{Z}-Z|^2. \tag{73}$$

Since (68_1) implies that $|X_s|, |Y_s|\leqq c_2$, the first inequality in (33_1) follows from (67) and (70_1). The second inequality in (33_1) follows from (69_2) and (70_2).

In order to prove (34_1), differentiate (72) with respect to $\sigma=\xi$ or $\sigma=\eta$. This gives

$$G_{js\sigma}=\gamma_{jX\Xi}X_s(W(z))X_t(W(\zeta))+\gamma_{jX\mathrm{H}}X_x(W(z))Y_t(W(\zeta))+\cdots, \tag{74}$$

where $t=x$ or $t=y$ according as $\sigma=\xi$ or $\sigma=\eta$, and $+\cdots$ indicates two more terms. When $j=1$, the first factor of the first term on the right is

$$\gamma_{1X\Xi}=1/|\mathbf{Z}-Z|^2-2(\Xi-X)^2/|\mathbf{Z}-Z|^4; \tag{75}$$

the other factors $\gamma_{1X\mathrm{H}}$, $\gamma_{1Y\Xi}$, $\gamma_{1Y\mathrm{H}}$ are similar. Thus the first inequality in (34_1) follows from (67), (68_1) and (70_1). If $j=1$ and if (74) is differentiated with respect to $e=a$, b, or c, then (70_2) shows that $\gamma_{1X\Xi e},\cdots$ have majorants of the form $c_2/|z-\zeta|^2$, while (69_1) and (69_2) show that $X_s, X_{se},\cdots$ have majorants of the form c_2. This proves (34_1).

In order to prove (35_1), let $j=1$ and let (74) be differentiated with respect to $t=x$ or $t=y$. It is clear that the resulting terms involving a third order partial derivative of γ (with respect to X, Y, Ξ, H) are majorized by $c_2/|z-\zeta|^3$, while, by (68_2), those involving a second order partial derivative of γ, and a second order partial derivative of X or Y, are majorized by $c_2/|z-\zeta|^2R$. Since $2R>|z-\zeta|$, the inequality (35_1) follows.

11. Proof of (33_2), (34_2), (35_2). The proofs of these inequalities will be similar to those of (33_1), (34_1), (35_2) but they will depend, in addition, to (68), (69) and (70), on two elementary inequalities and on some remarks on the inequalities (70) for the case when $|z|=R$ or $|\zeta|=R$. Both of the required elementary inequalities, which can be interpreted in terms of the geometry of the circle, will be proved for the sake of completeness.

The first elementary inequality is

$$R^{-1}|R^2-\bar{Z}\mathbf{Z}|\geqq|\mathbf{Z}-Z|/4, \qquad |Z|<R, |\mathbf{Z}|<R. \tag{76}$$

In order to verify (76), note that if Z_* is the mid-point of the line segment

joining Z and $R^2/\bar{Z}$, then $|Z_*| > R$. Hence, the perpendicular bisector of this segment does not intersect the circle $|Z| = R$. Consequently,

$$|\mathbf{Z} - R^2/\bar{Z}| \geqq |\mathbf{Z} - Z|.$$

But $R^{-1}|R^2 - \bar{Z}\mathbf{Z}| = |Z/R| \cdot |\mathbf{Z} - R^2/\bar{Z}|$, and so (76) holds if $|Z| \geqq \frac{1}{2}R$. On the other hand, if $|Z| < \frac{1}{2}R$, then $R^{-1}|R^2 - \bar{Z}\mathbf{Z}| \geqq \frac{1}{2}R \geqq |\mathbf{Z} - Z|/4$. This completes the verification of (76).

The second elementary inequality is

$$R(R - |\mathbf{Z}|)/|R^2 - \bar{Z}\mathbf{Z}| \leqq 2. \tag{77}$$

The proof of this is obvious if it is remarked that the left side does not exceed $|R/Z|$.

The derivations of the inequalities (68)-(70) show that they are valid if the arguments z, ζ, W of the functions involved are on the boundaries C, C, C_0 of the appropriate circular or elliptical domain. This fact will now be used to derive the following consequences of (70_1), (70_2), respectively:

$$c_2^{-1} \leqq (R - |Z(W(z))|)/(R - |z|) \leqq c_2, \tag{78_1}$$

$$|\partial(|Z(W(z))|^2 - R^2)/\partial e| \leqq c_2(R - |Z|) \qquad (e = a, b, \text{or } c). \tag{78_2}$$

In order to verify the second inequality in (78_1), let z be fixed ($|z| < R$) and let z_0 be a point of C nearest z. Thus $|z - z_0| = R - |z|$. Then $|Z(W(z_0))| = R$, and so

$$|Z(W(z)) - Z(W(z_0))| \geqq R - |Z(W(z))|.$$

The second inequality in (70_1) shows that the expression on the left is majorized by $c_2|z - z_0| = c_2(R - |z|)$. Hence the second inequality in (78_1) follows. The first inequality in (78_1) is similarly proved.

If R^2 is replaced by $|Z(W(z_0))|^2$, then (78_2) follows from the case $\zeta = z_0$ of (70_2) (and the fact that $||f|_e| \leqq |f_e|$).

The inequalities (77) and (78_1) will be used together, in the form

$$R(R - |\zeta|)/|R^2 - \bar{Z}\mathbf{Z}| \leqq c_1, \tag{79}$$

where Z and $\mathbf{Z}$ are given by (67).

Finally,

$$R^2 - \bar{Z}\mathbf{Z} = \Re + i\Im, \tag{80}$$

where $\Re$ and $\Im$ are real and are given by

$$\begin{aligned} \Re &= (R^2 - |\mathbf{Z}|^2) + \Xi(\Xi - X) + \mathrm{H}(\mathrm{H} - Y), \\ \Im &= \mathrm{H}(X - \Xi) + \Xi(\mathrm{H} - Y) \end{aligned} \tag{81}$$

or, equivalently, by

$$\mathfrak{R} = (R^2 - |Z|^2) + X(X - \Xi) + Y(Y - \mathrm{H}), \quad \mathfrak{J} = X(\mathrm{H} - Y) + Y(X - \Xi).$$

The proof of (33_2) can now proceed as follows:

In the case $j = 2$ of (72),

$$(82) \quad \gamma_{2X} = (-\Xi\mathfrak{R} + \mathrm{H}\mathfrak{J})/|R^2 - \bar{Z}\mathbf{Z}|^2, \quad \gamma_{2Y} = (-\mathrm{H}\mathfrak{R} - \Xi\mathfrak{J})/|R^2 - \bar{Z}\mathbf{Z}|^2.$$

Thus $|\gamma_{2S}| \leqq R/|R^2 - \bar{Z}\mathbf{Z}|$, where $S = X$ or $S = Y$. Hence the first inequality in (33_2) follows from (76) and (70_1).

In order to prove the second part in (33_2), note that a differentiation of (72), where $j = 2$, with respect to e $(= a, b$ or $c)$ leads to terms each of which is majorized by one of the expressions

$$c_2 R/|R^2 - \bar{Z}\mathbf{Z}|, \quad c_2 R^2 (R - |\mathbf{Z}|)/|R^2 - \bar{Z}\mathbf{Z}|^2, \quad c_2 R^2 |z - \zeta|/|R^2 - \bar{Z}\mathbf{Z}|^2,$$

by virtue of (81), (82) and (69), (70), (78). Hence the second inequality in (33_2) follows from (76) and (77).

This proof of (33_2) shows that (34_2), (35_2) can be proved in a manner similar to that used above for (34_1), (35_1), with $\mathfrak{R}$, $\mathfrak{J}$ in (81) playing the rôles of the real and imaginary parts, $\Xi - X$ and $\mathrm{H} - Y$, of $\mathbf{Z} - Z$. The details of these arguments will therefore be omitted.

Since the factor d^{-1} in (66) is simply the function $(ac - b^2)^{-\frac{1}{2}}$ of a, b, c, it is clear that Lemma 3 follows from the inequalities (33_j), (34_j), (35_j) for $j = 1, 2$.

12. Proof of Lemma 5. The function (45) can be written as $\mu(z_0, z_0)$, where

$$(83) \qquad \mu(z, z_0) = \iint_{\mathrm{D}} (l(\zeta) - l(z)) h(\zeta) L(\zeta, z; z_0) \, d\xi d\eta.$$

In order to prove Lemma 5, it is sufficient to verify inequalities of the type (46) for both

$$(84) \qquad |\mu(z, z_0) - \mu(z, z^0)|$$

and

$$(85) \qquad |\mu(z_2, z_0) - \mu(z_1, z_0)|.$$

The second inequality in (42) and the inequalities (38) and (44) show that (84) is majorized by

$$k_4 k_5 k_6 a(|z_0 - z^0|) \iint_{\mathrm{D}} a(|\zeta - z|) |\zeta - z|^{-2} d\xi d\eta.$$

The last integral does not exceed $2\pi \int_0^{2R} a(r)r^{-1}dr$. Hence

$$|\mu(z,z_0)-\mu(z,z^0)| \leqq 2\pi k_4k_5k_6 a(|z_0-z^0|)\int_0^{2R} a(r)r^{-1}dr. \tag{86}$$

In order to appraise (85), let

$$r=2|z_1-z_2| \tag{87}$$

and let $E=E(r)$ denote the portion of the circular disc $|z-z_1|<r$ contained in D,

$$E:\ |z-z_1|<r, |z|<R. \tag{88}$$

Then the difference whose absolute value occurs in (85) can be written as

$$\mu(z_2,z_0)-\mu(z_1,z_0)=I_1+I_2-(\Delta l)I_3, \tag{89}$$

with

$$I_1=\Delta\iint_E J(\zeta,z;z_0)\,d\xi d\eta,$$

$$I_2=\iint_{D-E}(l(\zeta)-l(z_1))h(\zeta)\Delta L(\zeta,z;z_0)\,d\xi d\eta, \tag{90}$$

$$I_3=\iint_{D-E} h(\zeta)L(\zeta,z_2;z_0)\,d\xi d\eta,$$

where $J(\zeta,z;z_0)$ is the integrand in (83) and, for any function $g(z,\cdots)$ depending on z, the symbol Δg denotes the difference $g(z_2,\cdots)-g(z_1,\cdots)$.

By (38), (44) and the first inequality in (42),

$$\iint_E |J(\zeta,z;z_0)|\,d\xi d\eta \leqq k_4k_5k_6\iint_E a(|\zeta-z|)|\zeta-z|^{-2}\,d\xi d\eta.$$

If ζ is on E and if $z=z_1$ or $z=z_2$, then $|z-\zeta|\leqq 2r$. Hence

$$|I_1|\leqq 2(k_4k_5k_6)(2\pi)\int_0^{2r} r^{-1}a(r)\,dr. \tag{91}$$

It follows from (43) that $|\Delta L|\leqq \frac{1}{2}k_5 r/|z_*-\zeta|^3$, where z_* is some point on the line segment joining z_1 and z_2. If ζ is not in E, then $|z_*-\zeta|\geqq |z_1-\zeta|-|z_1-z_*|$. Since $|z_1-z_*|\leqq \frac{1}{2}r\leqq \frac{1}{2}|z_1-\zeta|$, it follows that $|z_*-\zeta|\geqq \frac{1}{2}|z_1-\zeta|$. Hence $|\Delta L|\leqq 4k_5r/|z_1-\zeta|^3$. Thus, by (38) and (44),

$$|I_2| \leqq 4(k_4k_5k_6)(2\pi)r\int_r^{2R} r^{-2}a(r)\,dr. \tag{92}$$

Finally, (38) and the first inequality in (42) imply that

$$|I_3| \leqq k_4k_5 \iint_{\text{D-E}} |\zeta - z_2|^{-1}d\xi d\eta \leqq (k_4k_5)(2\pi)\int_{\frac{1}{2}r}^{2R} r^{-1}dr;$$

so that, by (44),

$$|(\Delta l)I_3| \leqq (k_4k_5k_6)(2\pi)a(\tfrac{1}{2}r)\log(4R/r). \tag{93}$$

By (89), (91), (92) and (93), the difference (85) is majorized by

$$K(k_4k_5k_6)\{a(\tfrac{1}{2}r)\log(4R/r) + \int_0^{2r} r^{-1}a(r)\,dr + r\int_{\frac{1}{2}r}^{2R} r^{-2}a(r)\,dr\},$$

where $\frac{1}{2}r = |z_1 - z_2|$. Hence, Lemma 5 follows from (86), by virtue of the definition of $\beta^2(r)$ in the formula line following (46).

13. An example. Let $F = F(r)$ be a continuous function on $0 \leqq r \leqq R$ satisfying

$$F(r) \gtrless 0 \text{ according as } r \gtrless 0 \tag{94}$$

and let S be the surface of revolution defined by

$$S\colon\ z = z(x,y) = \int_0^r F(r)\,dr \qquad (r = (x^2+y^2)^{\frac{1}{2}} \geqq 0). \tag{95}$$

(In this section, z is real and (x,y,z) are coordinates in space.) Thus S is a surface of class C^1. The element of arc-length on S is given by (7), where

$$g_{11} = 1 + F^2x^2/(x^2+y^2), \qquad g_{12} = F^2xy/(x^2+y^2), \tag{96}$$
$$g_{22} = 1 + F^2y^2/(x^2+y^2).$$

Let $a = a(r)$ be defined, for $0 \leqq r \leqq \frac{1}{2}$, by

$$a(r) = 1/\log^2 r \text{ or } a(r) = 0 \text{ according as } r \gtrless 0 \tag{97}$$

and let

$$F(r) = -1/\log r \text{ or } F(r) = 0 \text{ according as } r \gtrless 0. \tag{98}$$

Then (97) satisfies (3) and $f = F^2$ satisfies (2) on $x^2 + y^2 \leqq R^2$ $(\leqq 1/4)$.

It is easily verified that $f = g_{ik}$ also satisfy (2)-(3) for $i, k = 1, 2$, where g_{ik} is given by (96) and $a(r)$ by (97).

A mapping $u = u(x, y)$, $v = v(x, y)$ of class C^1 transforming (7) into the conformal normal form is given by

$$u = \rho(r)x, \qquad v = \rho(r)y, \qquad r = (x^2 + y^2)^{\frac{1}{2}}, \tag{99}$$

where, for $r > 0$,

$$\rho(r) = r^{-1} \exp\left(-\int_r^R r^{-1}(1 + F^2(r))^{\frac{1}{2}} dr\right); \tag{100}$$

the conformal normal form (8) for ds^2 is

$$ds^2 = \rho^{-2}(r)\,(du^2 + dv^2); \tag{101}$$

cf. [3], Appendix. The definition of $\rho(0)$ follows by continuity from (102) below; the fact that u, v are of class C^1 can be seen from the derivation of (102); finally, $\partial(u, v)/\partial(x, y) \neq 0$ is a consequence of $\rho > 0$.

Note that (100) satisfies $R\rho(r) = \exp \int_r^R \{r^{-1}(1 - (1 + F^2(r))^{\frac{1}{2}}\} dr$; so that

$$R\rho(r) = \exp\left(\int_0^R - \int_0^r\right) = \text{Const.} \exp - \int_0^r, \quad \text{where Const.} = \exp \int_0^R.$$

On writing $(1 + F^2)^{\frac{1}{2}}$ as $1 + \frac{1}{2}F^2(r) + \cdots$, it is seen that

$$(\text{Const.}/R)\rho^{-1}(r) = \exp \int_0^r (\tfrac{1}{2} r^{-1} F^2(r) + \cdots) dr.$$

Since $\int_0^r r^{-1} F^2(r)\, dr = -1/\log r$, by (98), it follows that

$$\rho^{-1}(r) = (R/\text{Const.})\{1 - \tfrac{1}{2}(1 + o(1))/\log r)\}. \tag{102}$$

Hence, the factor $\rho^{-2}(r)$ in (101) satisfies, for small $r > 0$,

$$\rho^{-2}(r) - \rho^{-2}(0) \geqq (\tfrac{1}{2}R/\text{Const.})^2(-1/\log r). \tag{103}$$

By the transformation rule for a metric tensor, there exists a constant $c > 0$ such that at least one of the four partial derivatives $f = u_x, u_y, v_x, v_y$ satisfies

$$|f(x, y) - f(0, 0)| \geqq c/|\log r|. \tag{104}$$

On the other hand, the $\beta(r)$ in (17) belonging to (97) satisfies $\beta(r) \leqq C/|\log r|$ for a suitable choice of $C = C(R)$. Hence, by Lemma 1, $f = u_x, u_y, v_x, v_y$ satisfy

$$|f(P) - f(Q)| \leqq C/|\log |PQ||. \tag{105}$$

This example shows that, in general, the function $\beta(r)$ in Lemma 1 cannot be replaced by a "smaller" function. It also shows that, while $\alpha(r)$ satisfies the Dini condition (3), the function $\beta(r)$ need not, and that $\beta(r)$ cannot be replaced by a function which satisfies a Dini condition

$$\int_{+0} r^{-1}\beta(r)\,dr < \infty.$$

As observed in Section 1, it follows that when (1) is relaxed to (2)-(3), the usual method of successive approximations cannot supply existence theorems.

The example of a ds^2 given by (96) is a modification of one given by Lavrentieff [12], p. 420, and used in [3], Appendix, for a related purpose.

[In the last formula line of [3], p. 308, the term $x/2R$ should be $x^2/2R$.]

14. Remarks on the proof of (**). It is clear from the proof of (*) that the terms Du, E, those which occur in (15), but not in (11), cause no complications and that the proof of the main (non-parenthetical) part of (**) follows from that of Lemma 2. In fact, the same is true even if Du in (15) is replaced by $F_1u_x + F_2u_y + Du$, when D, F_1, F_2 are continuous. In this case, however, R_0 will depend also on the bounds for $|F_1|$, $|F_2|$.

Since analogous remarks apply to the last (parenthetical) part of (**), the proof of this part of (**) will be indicated only for the case (11) of (15), where $D = E = 0$. It will be shown that, under the conditions stated, the proof of Lemma 1 can be modified so as to lead to an a priori estimate for the degree of continuity, and to a priori bounds, for the second order partial derivatives of C^2-solutions $u = u(x, y)$ of (11).

To this end, consider the integro-differential equation (52) for w $(= u - \phi)$. Differentiation of (52) with respect to $s = x$ or $s = y$ leads to

$$2\pi w_s(z) = \iint_D h(\zeta)\, G_s(\zeta, z; a_0, b_0, c_0)\, d\xi d\eta. \tag{106}$$

This step can be made, since it is assumed that A, B_1, B_2, C are of class C^1 and that u, ϕ are of class C^2.

Since A, B_1, B_2, C are of class C^1, it follows from (*) that w_x, w_y satisfy a uniform Hölder condition of any order $\lambda < 1$ (with a Hölder constant

depending only on λ, R_0 and the bounds for the partial derivatives of A, B_1, B_2, C). Hence, the motivation for (53) assures the validity of the formal differentiation of (106) with respect to $t=x$ or $t=y$ at the point $z=z_0$,

$$(107)\qquad 2\pi w_{st}(z_0)=h(z_0)(\iint_D G_s d\xi d\eta)_t+\iint_D (h(\zeta)-h(z_0))G_{st}d\xi d\eta,$$

where the argument of the partial derivative of G in the last integral is $(\zeta, z_0; a_0, b_0, c_0)$. In fact, this motivation is more readily seen if the terms h_{2x}, h_{2y} in h are written as

$$h_{2x}=A_x(w+\phi)_x+(A-A_0)(w+\phi)_{xx}+\cdots,$$
$$h_{3y}=B_{2y}(w+\phi)_x+(B_2-B_{20})(w+\phi)_{xy}+\cdots.$$

Since Lemma 3 holds if $\sigma=x$ or $\sigma=y$ (as well as $\sigma=\xi$ or $\sigma=\eta$ in (34)-(35)), the last formula and (107) show that, if R is sufficiently small, then the arguments leading to Lemma 1 supply a priori estimates for the degree of continuity and a priori bounds for w_{st}. The proof of Lemma 2 shows that under the assumptions of the last part of (**), C^1-solutions of (11) are of class C^2.

APPENDIX.

Potential Theory and Lebesgue Constants.

Let $f=f(x,y)$ be uniformly continuous on an open bounded domain D of the (x,y)-plane. Then a *formal* solution $\phi=\phi(x,y)$ of Poisson's equations

$$(1)\qquad \phi_{xx}+\phi_{yy}=f$$

on D is the logarithmic potential

$$(2)\qquad \phi(x,y)=\tfrac{1}{2\pi}\iint_D f(u,v)\log r\,dudv,$$

where $r^2=(x-u)^2+(y-v)^2$. Actually, the second derivatives of the function (2) need not exist on D if $f(x,y)$, instead of satisfying something like a Hölder condition, is just uniformly continuous. In fact, Petrini [15], pp. 132-133, has shown that the derivative ϕ_{xx} of (22) will exist at a point (a,b) of D if and only if the limit

$$(3)\qquad \lim_{\epsilon\to 0}\iint_{D-E(\epsilon;a,b)} f(u,v)\,(\log r)_{uu}\,dudv \text{ exists},$$

where $E(\epsilon; a, b)$ denotes the interior of the circle of radius ϵ about (a, b), and that a corresponding criterion holds for ϕ_{yy} and ϕ_{xy} (or ϕ_{yx}), with $(\log r)_{uu}$ replaced by $(\log r)_{vv}$, $(\log r)_{uv} = (\log r)_{vu}$ in (3). (Incidentally, this implies that $\phi_{xy}(a, b)$ exists if and only if $\phi_{yx}(a, b)$ does [and is $\phi_{yx}(a, b)$]; in addition [cf. *loc. cit.*, p. 134], the existence of $\phi_{xx}(a, b)$ is equivalent to that of $\phi_{yy}(a, b)$).

Petrini observes ([15], p. 138) that if D contains $(0, 0)$ and if

$$f(x, y) = x^2/(r^2 \log r) \qquad \text{(if } (x, y) \neq (0, 0), \text{ and } f(0, 0) = 0), \tag{4}$$

then (3) fails to hold at $(a, b) = (0, 0)$. This proves that the second derivatives of (2) need not exist when f is just continuous.

Another turn to Petrini's criterion (3) was given in [17]. This turn, which in [17] made possible the passage from (1) to the homogeneous equation

$$\psi_{xx} + \psi_{yy} + f\psi = 0 \tag{5}$$

(and which was further exploited in [7]), consists in the following observation: Instead of finding an explicit example (such as (4)) which violates Petrini's condition (3), it is sufficient to think of the limit (3) (if any) as a "singular integral" in the sense of Lebesgue, with

$$\iint_{D-E(\epsilon; a, b)} |(\log r)_{uu}| \, dudv \tag{6}$$

as the "ϵ-th Lebesgue constant." Since (6) tends to ∞ as $\epsilon \to 0$, it is sufficient to appeal to Lebesgue's classical "norm construction" (cf. his *Leçons sur les séries trigonométriques* (1906), pp. 85-87) in order to obtain a uniformly continuous $f(x, y)$ for which the logarithmic potential (2) fails to possess second derivatives.

The object of this appendix is to point out the fact that *there exist on D (say on $x^2 + y^2 < 1$) uniformly continuous functions $f(x, y)$ corresponding to which the second derivatives*

$$\phi_{xx}, \ \phi_{xy} = \phi_{yx}, \ \phi_{yy} \tag{7}$$

of the logarithmic potential (2) *exist on D but* (2) *fails to be of class C^2 in any neighborhood of certain points of D (so that the derivatives* (7) *exist but are not continuous*). In addition, the steps leading to this fact will make it clear that it can be transferred from (1) to (5), if use is made of the considerations applied in [17].

The above-quoted passage in Lebesgue's book is that which, from the

unboundedness of the Lebesgue constants of the partial sums of Fourier series, constructs the existence of a continuous function having a divergent Fourier series. But a later passage (Lebesgue, *op. cit.*, pp. 88-89) constructs, on the same basis, a continuous (periodic) function having a Fourier series which is convergent throughout but does not converge uniformly. The statement italicized above follows by using this *second* construction of Lebesgue (instead of appealing, as in [17], to his *first* construction, that in *op. cit.*, pp. 85-87).

It may be mentioned that, while (3) is necessary and sufficient for the existence of $\phi_{xx}(a,b)$, *the uniform existence of the limit* (3) *on all compact subsets of points* (a,b) *of* D *is necessary and sufficient for the existence of a continuous* ϕ_{xx}. In fact, this statement follows from the considerations of [15], pp. 131-133, leading to (3), and from the fact that a function of a single variable has a continuous derivative if and only if the difference quotients have a uniform limit.

Similar remarks hold for the existence and continuity of $\phi_{xy} = \phi_{yx}$ and ϕ_{yy}. The nature of these criteria for the existence and continuity of (7) is one of the reasons why, in contrast to a simple "explicit" example (such as (4)) for the non-existence of (7), a "construction" is needed to exhibit a case in which (7) exist but are not continuous.

These criteria also show that the "construction" can be carried out so as to lead to bounded, but not continuous, functions (7).

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] L. Bianchi, *Opere*, vol. 1_2 (Rome, 1953), pp. 123-135 [1889].

[2] S. S. Chern, "An elementary proof of the existence of isothermal parameters on a surface," (to appear in the Proceedings of the American Mathematical Society).

[3] ———, P. Hartman and A. Wintner, "On isothermic coordinates," *Commentarii Mathematici Helvetici*, vol. 28 (1954), pp. 301-309.

[4] U. Dini, *Serie di Fourier ed altre rappresentazioni analitiche delle funzioni di una variabile reale*, Pisa, 1880.

[5] ———, "Sur la méthode des approximations successives pour les équations aux dérivées partielles du deuxième ordre," *Acta Mathematica*, vol. 25 (1902), pp. 185-230.

[6] P. Hartman and A. Wintner, "On the fundamental equations of differential geometry," *American Journal of Mathematics*, vol. 72 (1950), pp. 757-774.

[7] ——— and A. Wintner, "On the existence of Riemannian manifolds which cannot carry non-constant analytic or harmonic functions in the small," *ibid.*, vol. 75 (1953), pp. 260-276.

[8] O. Hölder, *Beiträge zur Potentialtheorie*, Inaugural-Dissertation (Tübingen), Stuttgart, 1882.

[9] E. Hopf, "Über den funktionalen, inbesondere den analytischen Charakter der Lösungen elliptischer Differentialgleichungen zweiter Ordnung," *Mathematische Zeitschrift*, vol. 34 (1932), pp. 194-233.

[10] A. Korn, "Über Minimalflächen, deren Randkurven wenig von ebenen Kurven abweichen," *Abhandlungen der Königlich Preussischen Akademie der Wissenschaft*, Berlin (1909), Anhang II.

[11] ———, "Zwei Anwendungen der Methode der sukzessiven Annäherungen," *Schwarz Festschrift*, Berlin (1914), pp. 215-229.

[12] M. Lavrentieff, "Sur une classe de représentations continues," *Recueil Mathématique*, vol. 42 (1935), pp. 407-424.

[13] L. Lichtenstein, "Zur Theorie der konformen Abbildung. Konforme Abbildung nicht-analytischer, singularitätenfreier Flächenstücke auf ebene Gebiete," *Bulletin International de l'Académie des Sciences de Cracovie*, ser. A, 1916, pp. 192-217.

[14] ———, "Neuere Entwicklung der Theorie partieller Differentialgleichungen zweiter Ordnung vom elliptischen Typus," *Encyklopädie der mathematischen Wissenschaften*, vol. IIC (1924), pp. 1279-1334.

[15] H. Petrini, "Les dérivées premières et secondes du potentiel logarithmique," *Journal de Mathématiques*, ser. 6, vol. 5 (1909), pp. 127-223.

[16] H. A. Schwarz, *Gesammelte mathematische Abhandlungen*, vol. 2 (1890), pp. 102-107 [1869].

[17] A. Wintner, "On the Hölder restrictions in the theory of partial differential equations," *American Journal of Mathematics*, vol. 75 (1950), pp. 731-738.

ON ALGEBRAIC GROUPS OF TRANSFORMATIONS.*

By André Weil.

In my *Variétés abéliennes* (Hermann, Paris, 1948; quoted hereafter as VA), I gave the rudiments of a theory of algebraic group-varieties. As these have become wholly inadequate to the present state of growth of algebraic geometry, a fuller treatment of this topic will be given here.

To define a group in algebraic geometry, one simply takes over the usual definition and adds the condition that all the objects entering into it must have a meaning from the point of view of the algebraic geometer. This means that the elements of the group must be the points of algebraic varieties in finite number, that the mappings $(x, y) \to xy$ and $x \to x^{-1}$ which define the group-structure are mappings in the sense of algebraic geometry, i.e. that their graphs consist of algebraic varieties, and finally that these mappings are everywhere defined in the sense of algebraic geometry. The same can be done in an obvious manner for groups of transformations and for homogeneous spaces.

For simplicity, we consider only groups and spaces consisting of a single variety; this corresponds to the assumption of connectedness in the theory of topological groups. In § I, we shall deal with those properties of groups and transformation-spaces which are birationally invariant, giving what will eventually prove to be a birationally invariant characterization of such spaces; this is obtained by writing down the basic axioms for groups and transformation-spaces at generic points only. Our main purpose is, starting from such objects, to derive from them birationally equivalent objects which are groups and transformation-spaces in the full sense described above. The method which will be followed is very simple, and, I believe, the most natural one which could be imagined; it derives from the observation that the varieties from which one starts, even though they may not be true groups or transformation-spaces, nevertheless contain large pieces or "chunks" (more precisely, open subsets) of such spaces; to isolate these is the purpose of § II. In § III, they are pieced together, by the technique of "abstract varieties," so as to achieve the desired result; the way in which this is done at first

---

* Received December 27, 1954.

requires an enlargement of the groundfield. Then a modified procedure is given whereby our spaces can be exhibited as varieties over the original groundfield; according to an idea which was first applied to similar problems by Matsusaka, and again quite recently by Chow, this is done by building up suitable symmetric products by means of the Chow points of 0-cycles. Some auxiliary results, belonging to the foundations of algebraic geometry, which would have interrupted the treatment of the main topic, are dealt with in an Appendix. A further paper, to appear in this same volume, will contain various applications of the general theory.

§ I. Some birationally invariant results.

The very convenient language of the Zariski topology will be used freely in the following manner. By a *closed subset of a variety* V, or by a *closed set on* V, we shall understand any union of subvarieties of V, *other than* V; thus V itself is not a closed set on V; there is some impropriety in this (the proper words for our concept being "non-dense closed set"), but this seemed preferable to endless repetitions. An *open set on* V is defined as the complement of a closed set on V (this should properly be called a "non-empty open set"). If k is a field of definition for V, we say that a subset of V is *k-closed* if it is closed and its components are algebraic over k, and if moreover it is invariant by all automorphisms over k of the algebraic closure $\bar{k}$ of k. A *k-open set on* V is the complement of a k-closed set.

By a variety, we mean an abstract variety unless the contrary is stipulated. The final models for our groups and transformation-spaces will be constructed in §§ III-IV as abstract varieties; until then, little or nothing would be lost (and nothing would be gained) if we confined our attention to projective or to affine varieties.

1. Let V be a variety, defined over a field k. Let f be a mapping of $V \times V$ into V, defined over k. Consider the following condition on f:

(G1) *If x, y are independent generic points of V over k, and $z = f(x, y)$, then $k(x, y) = k(x, z) = k(y, z)$.*

This is equivalent to saying that $k(x) \subset k(z, y)$ and $k(y) \subset k(x, z)$. It implies that any two of the points x, y, z are independent generic points of V over k and determine the third one uniquely.

Let x, y, t be independent generic points of V over k; (G1) implies that

$(f(x,y),t)$ and $(x,f(y,t))$ are two pairs of independent generic points of V over k. Thus, if (G1) is assumed, the following condition is meaningful:

(G2) *If x, y, t are independent generic points of V over k, then:*

$$f(f(x,y),t) = f(x,f(y,t)).$$

This is of course the associativity condition (but postulated only at independent generic points) for f.

If (G1), (G2) are satisfied, we say that f is a *normal* (internal) *law of composition* on V, and that V, with this law, is a *pre-group*; f will then mostly be written as a multiplication, i.e. as xy instead of $f(x,y)$. If V, with the law f, is a pre-group over k, it is so, a fortiori, over every field K containing k. Let a variety V' be birationally equivalent to V over such a field K; let x,y be independent generic points of V over K, put $z=xy$, and call x',y',z' the generic points of V' over K which correspond to x, y, z respectively. Then $K(x')$, $K(y')$, $K(z')$ are respectively the same as $K(x)$, $K(y)$, $K(z)$, and thus, since $K(z') \subset K(x',y')$, we may write $z'=f'(x',y')$, where f' is a mapping of $V' \times V'$ into V', defined over K. One sees at once that f' satisfies (G1) and (G2); we say that it is the law of composition on V', derived from f by transfer; and we say that V', with the law f', is a pre-group *birationally equivalent* to the pre-group V with the law f. This shows that the concept of a pre-group is invariant under arbitrary birational correspondences; a pre-group can thus be studied on any model, e.g. on an affine or a projective model.

PROPOSITION 1. *Let V be a pre-group, defined over k. There is a uniquely determined mapping ϕ of V into V, which is defined over k and is such that, if we put $s^{-1}=\phi(s)$ for every s on V at which ϕ is defined, the following conditions are fulfilled whenever x, y are independent generic points on V over k:*

(i) $k(x^{-1}) = k(x)$; (ii) $(x^{-1})^{-1} = x$; (iii) $y = (x^{-1})(xy)$;

(iv) $x = (xy)(y^{-1})$; (v) $(xy)^{-1} = (y^{-1})(x^{-1})$.

If we put $z=xy$, we have $k(y) \subset k(x,z)$, and therefore there is a mapping λ of $V \times V$ into V, defined over k, such that $y=\lambda(x,z)$; similarly there is a mapping μ of $V \times V$ into V, defined over k, such that $x=\mu(z,y)$. Take t generic on V over $k(x,y,z)$; put $y'=yt$, $z'=zt$; by associativity, the latter relation gives $z'=xy'$. Put $u=\mu(y,z)$; by the definition of μ, this is equivalent to $y=uz$. By (G1), this implies that $k(u,z)=k(y,z)$, and so u, z, t are independent generic points on V over k; therefore, by (G2),

we have $(uz)t = u(zt)$, which can be written as $y' = uz'$; as this also shows that u, z' are generic and independent over k, the latter relation implies, by (G1), that $k(u) \subset k(y', z')$. Therefore $k(u)$ is contained in $k(y, z)$, i.e. in $k(x, y)$, and also in $k(y', z')$, i.e. in $k(x, y')$. But, by (G1), y and $y' = yt$ are generic and independent over $k(x)$, and so $k(x, y)$ and $k(x, y')$ are independent regular extensions of $k(x)$; their intersection is therefore $k(x)$, and so we have $k(u) \subset k(x)$, so that we may write $u = \phi(x)$, where ϕ is a mapping of V into V, defined over k. As x, u are no other than $\mu(z, y)$ and $\mu(y, z)$, the relation between them is symmetrical, and we have $x = \phi(u)$ and $k(x) \subset k(u)$, and so $k(x) = k(u)$. We have thus verified (i), (ii), (iii). Also, by (G1), any two of the points x, y, z in $z = xy$ determine the third one uniquely provided they are generic and independent over k; from this it follows that $u = \phi(x)$ is uniquely determined by the relation $y = uz$, and so the function ϕ is uniquely determined by (iii). From now on, write x^{-1} instead of $\phi(x)$.

Let now v be generic on V over $k(x, y)$; put $s = (xy)v = x(yv)$. As x, yv are generic and independent over k, $s = x(yv)$ is equivalent to $yv = x^{-1}s$, by (iii); and again by (iii), this is equivalent to $v = y^{-1}(x^{-1}s)$ since y and yv are generic and independent over k by (G1). By (i), the points x^{-1}, y^{-1} and v are generic and independent over k, and therefore the last relation, by (G2) can be written as $v = (y^{-1}x^{-1})s$. As $s = (xy)v$, and xy, v are generic and independent over k, this shows that $y^{-1}x^{-1} = (xy)^{-1}$, which is (v). This, with $z = xy$, can be written as $z^{-1} = y^{-1}x^{-1}$, which, by (iii), is equivalent to $x^{-1} = y(z^{-1})$; applying (v) to the latter relation, we get $x = (z^{-1})^{-1}(y^{-1})$, which, in view of (ii), gives (iv). This completes the proof.

With the same notations as above, we have $\lambda(x, z) = x^{-1}z$ and $\mu(z, y) = zy^{-1}$. One should observe, however, that the function λ may be defined at a point (s, t) of $V \times V$ without the expression $s^{-1}t$ being defined; in fact, λ may be defined at (s, t) without ϕ being defined at s. A similar remark applies to μ.

COROLLARY. *With the notations of* Prop. 1, *assume that the function* $f(x, y) = xy$ *is defined at* (x^{-1}, x). *Then the function* $x \to (x^{-1})x$ *is a constant* e, *rational over* k. *If, moreover,* f *is defined at* (e, x), *then* $ex = x$; *if it is defined at* (x, e), *then* $xe = x$.

With x, y and $z = xy$ as before, the assumption implies that $z^{-1}z$, i.e. (by Prop. 1(v)) $(y^{-1}x^{-1})z$ is defined. In the relation $(uv)z = u(vz)$, with u, v generic and independent over $k(z)$, specialize (u, v) to (y^{-1}, x^{-1}) over $k(z)$; by our assumption, the left-hand side is defined; also, u and vz get

specialized to y^{-1} and $x^{-1}z$, the latter being defined and equal to y by Prop. 1(iii). Since, by our assumption, f is defined at (y^{-1}, y), this gives $z^{-1}z = y^{-1}y$; in other words, the function $x^{-1}x$ has the same value at z and at y. As y, z are independent generic points of V over k, this implies that the function is a constant; as it is defined over k, its constant value must then be rational over k. Putting $e = x^{-1}x$ and replacing x by x^{-1}, we get, in view of Prop. 1(i)-(ii), $e = x(x^{-1})$. Taking t generic over $k(x, y)$, specialize t to x^{-1} in the relation $t(xy) = (tx)y$; the left-hand side becomes y by Prop. 1(iii), and the right-hand side becomes ey provided this is defined. Specializing y to x^{-1} in the same relation, we get $te = t$ provided te is defined.

2. Let V and W be two varieties, defined over a field k. Let f, g be two mappings, both defined over k, of $V \times V$ into V and of $V \times W$ into W, respectively. Consider the following conditions:

(TG1) *For a generic x over k on V, the mapping $u \to g(x, u)$ of W into W is a birational correspondence between W and W.*

This is equivalent to saying that, if x, u are independent generic points of V and of W, respectively, over k, then $k(x, g(x, u)) = k(x, u)$.

(TG2) *If x, y, u are independent generic points of V, V and W, respectively, over k, then $g(f(x, y), u) = g(x, g(y, u))$.*

If (TG1) is fulfilled, (TG2) is meaningful, since in that case $g(y, u)$ is generic on W over $k(x)$, while $f(x, y)$ is generic on V over $k(u)$ by (G1).

When (G1, 2) and (TG1, 2) are satisfied, we shall say that g is a *normal* (external) *law of composition* on W with respect to the pre-group V, and that W, with this law, is a *pre-transformation space* with respect to V; g will then mostly be written as a multiplication, i.e. as $g(x, u) = xu$; then (TG1), (TG2) appear as $k(x, xu) = k(x, u)$ and $(xy)u = x(yu)$. Just as before, we note that the concept of a normal law is independent of the field of definition, which may be enlarged at will, and that it is birationally invariant; if V' is birationally equivalent to V, and W' to W, the laws f, g can be transferred in an obvious manner to V', W'; the pair V', W', with the laws f', g' obtained from f, g by transfer, is said to be *birationally equivalent* to the pair V, W with the laws f, g. In particular, W, just as V, may be replaced by an affine model.

Take x, y, u as in (TG2); put $z = xy$, $v = yu$. By (TG1), v is generic on W over $k(x)$; so is xv, again by (TG1); therefore $x^{-1}(xv)$ is defined. But (TG2) can be written as $zu = xv$, and so we have $x^{-1}(zu) = x^{-1}(xv)$.

As x^{-1}, z and u are independent generic points of V, V and W over k, we can apply (TG2) to the left-hand side, which is therefore equal to $(x^{-1}z)u$, i.e. to yu by Prop. 1(iii), i.e. to v. This proves $x^{-1}(xv) = v$; as x, v are independent generic points of V, W over k, this must therefore remain true for any pair of such points.

The conditions stated above may be strengthened by assuming "generic transitivity," which means the following condition:

(H) *If x, u are independent generic points of V and of W, respectively, over k, then $g(x,u)$ is a generic point of W over $k(u)$.*

In that case, we say that W is a *pre-homogeneous space* with respect to the pre-group V. This condition is equivalent to saying that the graph of g on $V \times W \times W$ has the projection $W \times W$ on $W \times W$ (in the sense of my *Foundations*; the set-theoretic projection then contains a open subset of $W \times W$, by Prop. 10 of the Appendix).

3. The following result shows that a normal law of composition may be obtained from a mapping satisfying much weaker conditions than those stated above.

PROPOSITION 2. *Let V, W be two varieties, defined over a field k. Let g be a mapping of $V \times W$ into W, defined over k, satisfying* (TG1) *and the following condition:*

(TG2′) *There are two independent generic points x, y of V over k and a generic point z of V over k such that $g(z,u) = g(x, g(y,u))$ for u generic on W over $k(x,y,z)$.*

Let $k(\bar{x})$ be the smallest field of definition containing k for the mapping $u \to g(x,u)$ of W into W, $\bar{x}$ being a generic point over k of a variety $\bar{V}$. Then one can write $\bar{x} = \phi(x)$ and $g(x,u) = \bar{g}(\bar{x},u)$, where ϕ is a mapping from V to $\bar{V}$ and $\bar{g}$ a mapping from $\bar{V} \times W$ to W, both defined over k; putting $\bar{y} = \phi(y)$, $\bar{z} = \phi(z)$, we have $k(\bar{z}) \subset k(\bar{x}, \bar{y})$ and may write $\bar{z} = \bar{f}(\bar{x}, \bar{y})$, where $\bar{f}$ is a mapping from $\bar{V} \times \bar{V}$ to $\bar{V}$, defined over k. Finally, $\bar{f}$ and $\bar{g}$ satisfy the conditions (G1, 2), (TG1, 2) *and define $\bar{V}$ as a pre-group and W as a pre-transformation space with respect to $\bar{V}$.*

In the first place, the smallest field of definition containing k for $u \to g(x,u)$ is contained in $k(x)$ and is therefore, by Prop. 3 of the Appendix, a finitely generated regular extension of k; this may always be written as $k(\bar{x})$, e.g. by taking $\bar{x}$ as a suitable point in an affine space, which has then

a locus $\bar{V}$ over k and may be written as $\phi(x)$. As $g(x,u)$ is then rational over $k(\bar{x},u)$, it may be written as $\bar{g}(\bar{x},u)$, or more briefly as $\bar{x}u$; (TG2′) can then be written as $g(z,u)=\bar{x}(\bar{y}u)$, which shows that the function $u\to g(z,u)$ is defined over $k(\bar{x},\bar{y})$, so that $k(\bar{z})\subset k(\bar{x},\bar{y})$; we may then write $\bar{z}=\bar{f}(\bar{x},\bar{y})$, or more briefly $\bar{z}=\bar{x}\bar{y}$. It is clear that $\bar{g}$, $\bar{f}$ satisfy (TG1, 2); we have to show that $\bar{f}$ satisfies (G1, 2). By (TG1), if $v=g(x,u)$, the mapping $u\to v$ is a birational correspondence between W and W, defined over $k(\bar{x})$; its inverse must then be defined over the same field, so that we have $k(u)\subset k(\bar{x},v)$ and may write $u=h(\bar{x},v)$. Notations being as before, put $w=g(y,u)$; as this, by (TG1), is generic over $k(x)$ on W, the relation in (TG2′), which can be written as $\bar{z}u=\bar{x}w$, is equivalent to $w=h(\bar{x},\bar{z}u)$. This shows that the mapping $u\to w$ is defined over $k(\bar{x},\bar{z})$; since its smallest field of definition is $k(\bar{y})$, we get $k(\bar{y})\subset k(\bar{x},\bar{z})$. Similarly, we have $w=\bar{y}u$ and therefore $u=h(\bar{y},w)$; then the relation in (TG2′) can be written as $\bar{x}w=\bar{z}h(\bar{y},w)$, from which we conclude in the same manner that $k(\bar{x})\subset k(\bar{z},\bar{y})$. This shows that f satisfies (G1).

Now, if $\bar{x}_1$, $\bar{x}_2$ are any two generic points of $\bar{V}$ over k, there is an isomorphism σ of $k(\bar{x}_1)$ onto $k(\bar{x}_2)$ over k which maps $\bar{x}_1$ onto $\bar{x}_2$. Take u generic on W over $k(\bar{x}_1,\bar{x}_2)$, and put $u_1=\bar{x}_1u$, $u_2=\bar{x}_2u$. Then σ maps the graph of $u\to u_1$ onto the graph of $u\to u_2$. If $u_1=u_2$, these two functions coincide, and therefore, by Prop. 4 of F-IV$_2$, σ must induce the identity on the smallest field of definition of the first function. As this field is $k(\bar{x}_1)$, we have thus shown that $u_1=u_2$ implies $\bar{x}_1=\bar{x}_2$. Now let $\bar{x}$, $\bar{y}$, $\bar{t}$, u be independent generic points over k on $\bar{V}$, $\bar{V}$, $\bar{V}$, W; put $\bar{x}_1=(\bar{x}\bar{y})\bar{t}$ and $\bar{x}_2=\bar{x}(\bar{y}\bar{t})$, these being defined because $\bar{f}$ satisfies (G1). We have to show that $\bar{x}_1=\bar{x}_2$; by (G1), they are both generic over k on $\bar{V}$, and u is generic over $k(\bar{x}_1,\bar{x}_2)$ on W, so that we need only show that $\bar{x}_1u=\bar{x}_2u$. By (TG1), $\bar{x}(\bar{y}(\bar{t}u))$ is defined; by (TG2), this is the same as $(\bar{x}\bar{y})(\bar{t}u)$, which, again by (TG2), is the same as $\bar{x}_1u$ since $\bar{x}\bar{y}$, $\bar{t}$, u are independent generic points of $\bar{V}$, $\bar{V}$, W over k by (G1). Similarly $\bar{x}(\bar{y}(\bar{t}u))$ is the same as $\bar{x}((\bar{y}\bar{t})u)$ by (TG2), and this is the same as $\bar{x}_2u$ by (TG2) and (G1). This concludes the proof.

The external normal law of composition $\bar{g}$ constructed in Prop. 2 satisfies, in addition to (TG1, 2), the following condition:

(TG3) *If x is generic over k on V, $k(x)$ is the smallest field of definition containing k for the mapping $u\to g(x,u)$ of W into W.*

Whenever (TG3) is satisfied in addition to (G1, 2) (TG1, 2), we will say that V operates *faithfully* on W by g.

If V, W and a mapping g of $V \times W$ into W are given, and g satisfies (TG1, 2′, 3), then Prop. 2 shows that $(x, y) \to z$ (where x, y, z are the points of V which appear in (TG2′)) is a normal internal law of composition on V and that g is a normal external law with respect to the pre-group defined by f on V. In particular, if V, W, f and g are given and f, g satisfy (TG1, 2, 3), then f satisfies (G1, 2).

§ II. Construction of chunks.

4. Let V, W be a pre-group and a pre-transformation space and f, g the internal and external normal laws belonging to them, these being all defined over a field k; we will mostly write f, g multiplicatively, as has already been done in § I. Instead of saying that f is defined at a point (s, t) of $V \times V$, we shall frequently say that st is defined; similarly, when we say for instance that $s^{-1}((st)a)$ is defined, for s, t on V and a on W, this will mean the following: (i) f is defined at (s, t), with the value st; (ii) g is defined at (st, a), with the value $(st)a$; (iii) $x \to x^{-1}$ is defined at s, with the value s^{-1}; (iv) g is defined at $(s^{-1}, (st)a)$, with the value $s^{-1}((st)a)$. We recall that two expressions, built up from functions which are defined over k, coincide for all values of the variables for which they are both defined provided they are defined and coincide when the variables are given independent generic values over k. This applies for instance to the formulas in (G2) and (TG2) which express the associativity of f and g.

We say that V is a *group-variety* or a *group* if f is everywhere defined on $V \times V$ and $x \to x^{-1}$ is everywhere defined on V; then the corollary of Prop. 1 shows that there is a neutral element e on V with the usual properties. If V is a group, W will be called a *transformation-space* with respect to V if g is everywhere defined on $V \times W$; if, moreover, V operates transitively on W in the usual sense, i.e. if to every pair a, b on W there is an $s \in V$ such that $b = sa$, then W is called a *homogeneous space* with respect to V.

In § III, it will be shown that, to every pre-group V, there is a birationally equivalent group V', and that, to every pre-transformation space W with respect to V, there is a birationally equivalent transformation-space W' with respect to V'. The proof of this will include a proof of the fact that W is biregularly equivalent to an open subset of W' if and only if it fulfills the following condition:

(C) *If a is any point of W, and x a generic point of V over $k(a)$, then xa and $x^{-1}(xa)$ are defined.*

A pre-transformation space W with respect to V which fulfills this condition will be called a *chunk of transformation-space*, or more briefly a *chunk*.

For similar reasons, if W is a pre-homogeneous space, i.e. if g satisfies (H), we say that W is a *homogeneous chunk* if it satisfies (C) and the following:

(HC) *If a and x are as in* (C), *xa is generic over $k(a)$ on W.*

Finally, V itself will be called a *group-chunk* if it is a homogeneous chunk with respect to left-translations and if x^{-1} is everywhere defined on it, or in other words if it satisfies the following:

(GC1) *If s is any point on V, and x a generic point of V over $k(s)$, then xs and $x^{-1}(xs)$ are defined and xs is generic over $k(s)$ on V.*

(GC2) *For every s on V, s^{-1} is defined.*

PROPOSITION 3. *Call Ω the set of those points a on W such that xa and $x^{-1}(xa)$ are defined for x generic over $k(a)$ on V. Then Ω is a k-open subset of W; Ω and all k-open subsets of Ω are chunks; if $a \in \Omega$, we have $x^{-1}(xa) = a$, $k(x,a) = k(x,xa)$, and a is a point of the locus of xa over $k(a)$ on W.*

Call F the set of points on $V \times W$ where g is not defined; by Prop. 8 of the Appendix, this is a k-closed subset of $V \times W$. Let Γ be the graph of the mapping $(x,u) \to x^{-1}u$ of $V \times W$ into W, i.e. the locus of $(x,u,x^{-1}u)$ over k for x, u generic and independent over k on V, W. Call F' the k-closed subset of $V \times W \times W$ consisting of all points (x,u,v) with $(x,v) \in F$; let F'' be the union of the projections of the components of $\Gamma \cap F'$ on the product of the first two factors of $V \times W \times W$ (this being understood as in **F-IV**$_8$ and **F-VII**$_3$; F'' is the closure, in the Zariski topology, of the set-theoretic projection of $\Gamma \cap F'$ on $V \times W$; cf. Appendix, Prop. 10). It will now be shown that Ω is the same as the set Ω_1 of the points a on W such that $V \times a$ is not contained in $F \cup F''$. In fact, for xa to be defined, it is necessary and sufficient that $V \times a$ should not be contained in F; let Ω_0 be the set of points a with this property; it contains both Ω and Ω_1. If $a \in \Omega_0 - \Omega$, $x^{-1}(xa)$ is not defined; as x^{-1} is generic over $k(a)$ at the same time as x, this is equivalent to saying that $x(x^{-1}a)$ is not defined; as $x^{-1}a$ is defined, the point $(x,a,x^{-1}a)$ is then in $\Gamma \cap F'$, and therefore (x,a) is in F'', so that $V \times a \subset F''$ and $a \notin \Omega_1$. Conversely, if $a \in \Omega_0 - \Omega_1$, then (x,a) is in the projection of one of the components of $\Gamma \cap F'$, and so, if (y,u,v) is a generic point of that component over $\bar{k}$, (x,a) is a specialization of (y,u) over $\bar{k}$. As (y,u,v) is

on Γ and $x^{-1}a$ is defined, v has then the unique specialization $x^{-1}a$ over $(y,u)\to(x,a)$ with respect to $\bar{k}$; therefore $(x,a,x^{-1}a)$ is in F', and so $x(x^{-1}a)$ is not defined and a is not in Ω. This proves that $\Omega=\Omega_1$; the latter set being k-open by Prop. 7 of the Appendix, Ω is k-open.

As $x^{-1}(xu)=u$ for x, u generic and independent over k on V, W, we must have $x^{-1}(xa)=a$ whenever the left-hand side is defined, and so for $a\in\Omega$ and x generic over $k(a)$; this implies that $k(a)\subset k(x,xa)$, so that $k(x,a)=k(x,xa)$. Let y be generic over $k(x,a)$ on V; then (x^{-1},xa) is a specialization of (y,xa) over $k(x,a)$; as the former point is not in F, and F is k-closed, (y,xa) is not in F, and so $y(xa)$ is defined. As yx is generic over $k(a)$ by (G1) and is therefore a generic specialization of x over $k(a)$, $(yx)a$ is defined and is a generic specialization of xa over $k(a)$. By associativity, we have $y(xa)=(yx)a$ since both sides are defined; as $x^{-1}(xa)$ is defined, it is a specialization of $y(xa)$, and therefore also of $(yx)a$ and of xa, over $k(a)$. This shows that a is a specialization of xa over $k(a)$, i.e. that it is a point of the locus of xa over $k(a)$ on W. If now Ω' is any k-open subset of Ω, then the set $C=W-\Omega'$ is k-closed, and so, if xa is in C, a must be in C; in other words, if a is in Ω', so is xa; it is then clear that Ω' is a chunk.

The locus of xa over $k(a)$ could be described as the closure of the orbit of a under V on W.

COROLLARY. *Notations being as in Prop.* 3, *call* Ω_h *the set of the points* a *of* Ω *such that* W *is the locus of* xa *over* $k(a)$. *Then* Ω_h *is* k*-open or empty according as* W *is pre-homogeneous or not. In the former case,* Ω_h *and all* k*-open subsets of* Ω_h *are homogeneous chunks; and, if* a, b *are any two points of* Ω_h, *there are two generic points* x, y *of* V *over* $k(a,b)$ *such that* $xa=yb$.

Except for the last assertion, this is an immediate consequence of Prop. 11 of the Appendix, applied to the k-open set Ω of Prop. 3. Let now a, b be in Ω_h; take x, y generic on V over $k(a,b)$, and put $u=xa$, $v=yb$. Then the loci of u and of v over $k(a,b)$ are W, and so there is an isomorphism of $k(a,b,u)$ onto $k(a,b,v)$ over $k(a,b)$ which maps u onto v; this can be extended to an isomorphism σ of $k(a,b,x)$ onto some extension of $k(a,b,v)$; then x^σ is generic on V over $k(a,b)$ and we have $u^\sigma=x^\sigma a$, i.e. $x^\sigma a=yb$, so that x^σ and y satisfy the conditions stated in the corollary.

Finally, in order to construct a group-chunk from a given pre-group V, one need only observe that the graph V_1 of the function $x\to x^{-1}$ is a subvariety of $V\times V$, birationally equivalent to V, and that, if we transfer that function to V_1, we get an everywhere biregular birational correspondence between V_1 and itself since it is the same as the function induced on V_1 by the

mapping $(x, y) \to (y, x)$ of $V \times V$ onto itself. Therefore we may assume that we have started from a pre-group V on which x^{-1} was everywhere defined; had that not been the case, one would merely have had to replace V by V_1 to make it so. Call now Ω_h the set of the points $s \in V$ with the property stated in (GC1); by the corollary of Prop. 3, this is a k-open subset of V; as $x \to x^{-1}$ is an everywhere biregular mapping of V onto itself, it transforms Ω_h into a k-open set Ω_h^{-1}; then $\Omega_h \cap \Omega_h^{-1}$ is a group-chunk.

Thus we have constructed chunks for the three kinds of objects under consideration, viz., transformation-spaces, homogeneous spaces and groups. If W is a pre-transformation space, defined over k, the set W' of simple points on W is a k-open set on W; by applying Prop. 3 to W', we obtain a non-singular chunk. Similarly, one would get an everywhere normal chunk by taking for W' the set of points where W is normal, this being k-open by Corollary 3 of Prop. 8 of the Appendix. It will presently be seen that homogeneous chunks and in particular group-chunks are always non-singular, so that no special procedure is required to make them such.

By Corollary 2 of Prop. 8 of the Appendix, if one has constructed a chunk, one can at once derive from it a birationally equivalent chunk which is an affine variety; this also applies to homogeneous chunks. As to group-chunks, starting from a pre-group which we take to be an affine variety, and replacing it by the graph of the function x^{-1} on it, we get for our pre-group an affine model V on which x^{-1} is everywhere defined. Let V' be a k-open set on V which is a homogeneous chunk; let $x = (x_1, \cdots, x_m)$ be a generic point of V over k; take a polynomial P with coefficients in k which is 0 on $V - V'$ but not on V; as x^{-1} and $P(x)$ are everywhere defined functions on V, so is $P(x^{-1})$. Call V'' the locus of

$$(x_1, \cdots, x_m, 1/P(x), 1/P(x^{-1}))$$

over k in affine space; this is biregularly equivalent to the k-open subset determined on V by the inequalities $P(x) \neq 0$, $P(x^{-1}) \neq 0$. This is a group-chunk. We have thus proved the following:

PROPOSITION 4. *To every pre-homogeneous space* (resp. *pre-group*) *defined over k, there is a birationally equivalent homogeneous chunk* (resp. *group-chunk*) *which is an affine variety, defined over k. To every pre-transformation space W and every point a on W with the property stated in* (C), *there is a birationally equivalent chunk W' which is an affine variety and is such that the birational correspondence between W and W' is biregular at a; if a is simple on W, W' may be taken non-singular; if W is normal at a, W' may be taken everywhere normal.*

5. PROPOSITION 5. *Let V be a group-chunk and W a pre-transformation space with respect to V; let k be a field of definition for V, W. Then, if s is any point of V, and u a generic point of W over $k(s)$, su and $s^{-1}(su)$ are defined; the mapping $u \to su$ is a birational correspondence between W and itself; and $k(s,u) = k(s,su)$.*

Take x, y generic and independent on V over $k(s,u)$; put $y' = yx^{-1}$ and $u' = xu$; by (G1) and (TG1), y' and u' are generic and independent over k on V, W, so that $y'u'$ is defined; as we have shown $x^{-1}u'$ to be defined and equal to u, we get, by associativity, $y'u' = yu$. We now show that the expression obtained by substituting s for y in $y'u'$, i.e. in $(yx^{-1})(xu)$, is defined. In fact, since V is a group-chunk, the mapping $(z,t) \to t^{-1}z^{-1}$, where z, t are generic and independent over $k(s)$ on V, is defined at (s,t), and its value $t^{-1}s^{-1}$ at that point is generic over $k(s)$ on V; this implies that the mapping $(z,t) \to (t^{-1}z^{-1})^{-1}$ is also defined there; as this is only another expression for the mapping $(z,t) \to zt$, we conclude that the latter is defined at (s,t), i.e. that st is defined, and that st is generic over $k(s)$; substituting x^{-1} for t, this shows that $x' = sx^{-1}$ is defined and generic over $k(s)$ on V, and a fortiori that the mapping $y \to yx^{-1}$ of V into V is defined at s, with the value x'. The mapping $u \to u'$ is defined at u, with the value u' which is generic over $k(x,s)$ on W by (TG1). So x' and u' are generic and independent over k on V, W, and $x'u'$ is defined; more precisely, we have shown that the mapping $(y,u) \to y'u' = (yx^{-1})(xu)$ of $V \times W$ into W, which is defined over $k(x)$, is defined at (s,u). As this is only another expression for the mapping $(y,u) \to yu$, this implies that the latter is defined at (s,u), i.e. that su is defined, and that these mappings have the same value there, i.e. that $x'u' = su$. By (TG1), $x'u'$ is generic on W over $k(x,s)$; therefore su is generic on W over $k(s)$. But then our assumptions on s, u are also satisfied by s^{-1}, su, so that it follows from what we have already proved that $s^{-1}(su)$ is defined; its value must then be u, since $x^{-1}(xu) = u$, and so we have $k(u) \subset k(s,su)$, and therefore $k(s,u) = k(s,su)$; this means that $u \to su$ is a birational correspondence between W and W.

COROLLARY. *Assumptions being as in Prop. 5, assume also that V operates faithfully on W; let s, s' be any two points of V, and let u be generic on W over $k(s,s')$. Then $su = s'u$ implies $s = s'$.*

Take x generic over $k(s,s',u)$ on V. Since V is a group-chunk, xs is defined and generic over $k(u)$ on V; and su is defined and generic over $k(x)$ on W by Prop. 5; by associativity, this gives $(xs)u = x(su)$. Similarly we

have $(xs')u = x(s'u)$. Therefore $su = s'u$ implies $(xs)u = (xs')u$. But then we can repeat the argument used in the proof of Prop. 2; there is an isomorphism σ of $k(xs)$ onto $k(xs')$, mapping xs onto xs'; as this transforms the graph of the function $u \to (xs)u$ into itself, and as $k(xs)$ is the smallest field of definition for this graph because of the assumption of faithfulness, σ must be the identity, and $xs = xs'$. As $s = x^{-1}(xs)$ and $s' = x^{-1}(xs')$, this gives $s = s'$.

PROPOSITION 6. *Let V be a group-chunk and W a chunk of transformation-space with respect to V. Let s be any point on V and (a, b) any point on the graph of the birational correspondence $u \to su$ between W and itself; then the latter is biregular at (a, b), sa and $s^{-1}b$ are defined, and we have $sa = b$, $s^{-1}b = a$.*

We first show that sa is defined. Take x, y, u generic and independent on V, V, W over $k(a, b, s)$; and consider the mapping $(x, u) \to y^{-1}((yx)u)$, defined over $k(y)$, of $V \times W$ into W. By (GC1), $x \to yx$ is defined at s, with a value ys which is generic on V over $k(s, a)$. By (C), the mapping $(x, u) \to xu$ is defined at (ys, a), and so the mapping $(x, u) \to (yx)u$ is defined at (s, a), with the value $(ys)a$. At the same time, $(ys)u$ is defined since u is generic on W over $k(y, s)$, and $y(su)$ is defined because su is defined and generic over $k(y)$ by Prop. 5; by associativity, this gives $(ys)u = y(su)$. As (a, b) is on the graph of $u \to su$, and (u, su) is a generic point of that graph over $k(y, s)$, (a, b) is a specialization of (u, su) over $k(y, s)$; but then the relation $(ys)u = y(su)$ implies $(ys)a = yb$. By Prop. 3, the mapping $v \to y^{-1}v$ is defined at yb, i.e. at $(ys)a$, with the value b. We have thus proved that $(x, u) \to y^{-1}((yx)u)$ is defined at (s, a), with the value b; as this is but an expression for $(x, u) \to xu$, this shows that sa is defined and equal to b. Interchanging a, s with b, s^{-1}, and making use of Prop. 5, we see from this that $s^{-1}b$ is defined and equal to a. This implies a fortiori that the mappings $u \to su$, $u \to s^{-1}u$ are respectively defined at a, b, with values b, a; this means that the birational correspondence $u \to su$ is biregular at (a, b).

COROLLARY. *Every homogeneous chunk is non-singular.*

Let W be such a chunk with respect to a pre-group V; replace V by a birationally equivalent group-chunk. For any a on W, take x generic on V over $k(a)$; then $u \to xu$ is a birational correspondence between W and itself, transforming a into the generic point xa of W over $k(a)$, and biregular at a. As xa is simple on W, a must therefore be simple on W.

§ III. Construction of spaces.

From now on, until the end of § III, *V and W will denote respectively a group-chunk and a chunk of transformation-space with respect to V, both being at the same time assumed to be affine varieties; k will denote a common field of definition for V and W and for the normal laws given on them.*

6. Let n, n' be the dimensions of V, W, and take $N > 4n$ and also $> 3n + n'$; take N independent generic points $t_1, \cdots, t_N$ over k on V; put $K = k(t_1, \cdots, t_N)$. Let u be a generic point of W over K; put $S_\alpha = W$ and $u_\alpha = t_\alpha u$ for $1 \leqq \alpha \leqq N$. Take the u_α as the corresponding generic points of the varieties S_α over K; this defines birational correspondences $T_{\beta\alpha}$ between any two of the S_α; as we may write, by associativity, $u_\beta = (t_\beta t_\alpha^{-1}) u_\alpha$, $T_{\beta\alpha}$ is the birational correspondence $u \to (t_\beta t_\alpha^{-1}) u$ between W and itself. Proposition 6 of § II shows that $T_{\beta\alpha}$ is biregular at any pair of points on its graph. Therefore the varieties S_α (with empty "frontiers") and the $T_{\beta\alpha}$ may be used to define an abstract variety $\boldsymbol{S}$. Call $\bar{u}$ the generic point of $\boldsymbol{S}$ over K with the representatives u_α and write $\bar{u} = \Phi(u)$, $u = \Psi(\bar{u})$; Φ is a birational correspondence between W and $\boldsymbol{S}$, and Ψ is its inverse; both are defined over K. Let a be any point of W; by Prop. 4 of the Appendix, there is an α such that t_α is generic over $k(a)$; as W is a chunk, $t_\alpha a$ is then defined; this means that Φ is defined at a, $\Phi(a)$ being the point of $\boldsymbol{S}$ with the representative $t_\alpha a$ on S_α. As $t_\alpha^{-1}(t_\alpha a)$ is then defined and has the value a, Ψ is defined at the point $\Phi(a)$ with the value a. This shows that Φ is a biregular mapping of W onto its set-theoretic image $\Phi(W)$ on $\boldsymbol{S}$; as the latter is the set of points of $\boldsymbol{S}$ where Ψ is defined, it is K-open on $\boldsymbol{S}$ by Prop. 8 of the Appendix. Once and for all, we will agree to denote by $\bar{a}$ the image $\Phi(a)$ of $a \in W$ by Φ in $\Phi(W)$.

All this can be applied to the case when W is taken to be the same as V, V acting upon itself by left-translations. Let $\boldsymbol{G}$ be the abstract variety thus obtained from V; call Φ_0 the birational correspondence between V and $\boldsymbol{G}$ which takes the place of the mapping Φ defined above; and call Ψ_0 its inverse. We transfer to $\boldsymbol{G}$ the normal law on V by means of Φ_0; in other words, for x, y generic and independent on V over K and $\bar{x} = \Phi_0(x)$, $\bar{y} = \Phi_0(y)$, we define $\bar{x}\bar{y} = \Phi_0(xy)$, which implies $\bar{x}^{-1} = \Phi_0(x^{-1})$, and prove that this makes $\boldsymbol{G}$ into a group. In fact, the representative of $\bar{x}^{-1}$ on G_β is $t_\beta x^{-1} = (t_\beta x_\alpha^{-1}) t_\alpha$; if $\bar{s}$ is a point of $\boldsymbol{G}$ with a representative s_α on G_α, we can choose β such that t_β is generic on V over $k(s_\alpha, t_\alpha)$. Then, since V is a group-chunk, $t_\beta s_\alpha^{-1}$ is defined and generic on V over $k(s_\alpha, t_\alpha)$, and so $x \to (t_\beta x^{-1}) t_\alpha$ is defined

at s_α; this means that $\bar{s}^{-1}$ is defined and has a representative on G_β. Similarly, if we write $t = t_\gamma t_\alpha^{-1}$, the representative of $\bar{x}\bar{y}$ on G_γ is $t_\gamma xy = ((tx_\alpha)t_\beta^{-1})y_\beta$; let $\bar{r}$, $\bar{s}$ be two points of $\boldsymbol{G}$ with representatives r_α, s_β on G_α, G_β respectively; by Prop. 4 of the Appendix, we can choose γ so that t_γ is generic on V over $k(r_\alpha, s_\beta, t_\alpha, t_\beta)$; the same will then be true of t, and also of tr_α and of $(tr_\alpha)t_\beta^{-1}$ since V is a group-chunk; for a similar reason, this implies that $(x, y) \to ((tx)t_\beta^{-1})y$ is defined at (r_α, s_β), and this completes the proof that $\boldsymbol{G}$ is a group.

Now, going back to the space $\boldsymbol{S}$ constructed before, we transfer to $\boldsymbol{G}$, $\boldsymbol{S}$, by means of the birational correspondences Φ_0, Φ, the normal law given for V, W; in other words, for x, u generic and independent over K on V, W, and for $\bar{x} = \Phi_0(x)$, $\bar{u} = \Phi(u)$, we define $\bar{x}\bar{u} = \Phi(xu)$, and prove that this makes $\boldsymbol{S}$ into a transformation-space with respect to $\boldsymbol{G}$. In fact, the representative of $\bar{x}\bar{u}$ on S_γ is $((tx_\alpha)t_\beta^{-1})u_\beta$, where $t = t_\gamma t_\alpha^{-1}$ as before; the rest of the proof is then quite similar to the proof given above.

Naturally, if W is non-singular, $\boldsymbol{S}$ is non-singular; if W is everywhere normal, $\boldsymbol{S}$ is everywhere normal. Finally, if W is a homogeneous chunk, $\boldsymbol{S}$ is a homogeneous space. In fact, in that case, let $\bar{a}$, $\bar{b}$ be any two points of $\boldsymbol{S}$, with representatives a_α, b_β in S_α, S_β respectively. Take x generic over $K(\bar{a}, \bar{b})$ on V; put $\bar{x}' = \bar{x}\bar{a}$, $\bar{x}'' = \bar{x}\bar{b}$. For u generic over $K(x)$ on W, we have $\Psi(\bar{x}\bar{u}) = (xt_\alpha^{-1})u_\alpha$; as W is a homogeneous chunk, $x' = (xt_\alpha^{-1})a_\alpha$ is defined and generic over $K(\bar{a}, \bar{b})$ on W, and therefore we have $x' = \Psi(\bar{x}')$; similarly we have $x'' = \Psi(\bar{x}'')$ with $x'' = (xt_\beta^{-1})b_\beta$ generic over $K(\bar{a}, \bar{b})$ on W. That being so, there is an isomorphism of $K(\bar{a}, \bar{b}, x')$ onto $K(\bar{a}, \bar{b}, x'')$ over $K(\bar{a}, \bar{b})$ which maps x' onto x''; this can be extended to an isomorphism σ of $K(\bar{a}, \bar{b}, \bar{x})$ onto some extension of $K(\bar{a}, \bar{b}, x'')$. Then we have $\bar{x}^\sigma\bar{a} = \bar{x}'' = \bar{x}\bar{b}$, and so $\bar{b} = \bar{x}^{-1}\bar{x}^\sigma\bar{a}$.

7. From now on, it will be assumed that W and consequently $\boldsymbol{S}$ are everywhere normal. With this assumption, we shall construct an abstract variety $\boldsymbol{S}'$, defined over k, and a birational correspondence F between $\boldsymbol{S}'$ and W, also defined over k, so that the birational correspondence $\Phi \circ F$, defined over K, between $\boldsymbol{S}'$ and $\boldsymbol{S}$ is an everywhere biregular mapping of $\boldsymbol{S}'$ onto $\boldsymbol{S}$. This construction can then be applied to V itself, giving a variety $\boldsymbol{G}'$ and a birational correspondence F_0 between $\boldsymbol{G}'$ and V, both defined over k, such that $\Phi_0 \circ F_0$ is biregular between $\boldsymbol{G}'$ and $\boldsymbol{G}$. Transferring the normal laws for V, W to $\boldsymbol{G}'$, $\boldsymbol{S}'$ by means of F, F_0, we see that we have thus constructed a group $\boldsymbol{G}'$ and a transformation-space $\boldsymbol{S}'$, birationally equivalent to V, W over k; if W is pre-homogeneous and we have constructed $\boldsymbol{S}$ as a homogeneous space, $\boldsymbol{S}'$ will be a homogeneous space.

In constructing $\boldsymbol{S}'$, we may assume that V operates faithfully on W; in fact, if this were not so, one could replace V by another pre-group $\bar{V}$ satisfying this condition, according to Prop. 2 of § I, no. 3.

Notations will now be the same as in no. 6, with the additional assumptions that W and consequently $\boldsymbol{S}$ are everywhere normal, and that V acts faithfully on W, so that $\boldsymbol{G}$ acts faithfully on $\boldsymbol{S}$.

Let k' be any field containing k. Let $\sum_{i=1}^{r}(s_i)$ be a cycle of dimension 0 on V, rational over k', and assume that $s_i \neq s_j$ whenever $i \neq j$. Then, if we put $k'' = k'(s_1, \cdots, s_r)$, k'' is a Galois extension of k', i. e. separably algebraic and normal over k'. Call K'' the compositum of K and k''; let u be a generic point of W over K'', and put $w_i = s_i u$. If m is the dimension of the ambient affine space to W, we write $w_i = (w_{i1}, \cdots, w_{im})$. Put now

$$(1) \qquad y(T, U) = \prod_{i=1}^{r} (T - \sum_{\mu=1}^{m} w_{i\mu} U_\mu)$$

where $T, U_1, \cdots, U_m$ are indeterminates; let y be the point, in an affine space of suitable dimension, whose coordinates are all the coefficients of the homogeneous polynomial $y(T, U)$ except that of T^r; this is the so-called "Chow point" of the cycle $\sum_i (w_i)$, and $y(T, U)$ is its "Chow form."

As V acts faithfully on W, and the s_i have been assumed to be distinct, the corollary of Prop. 5, § II, no. 5, shows that the w_i are all distinct. We can therefore apply to them the following general result:

LEMMA. *If in* (1) *we take the w_i to be any set of distinct points, and k_0 is the prime field, then the w_i are separably algebraic over $k_0(y)$.*

By F-I$_5$, Th. 1, we need only show that a derivation D of the field $k_0(w_1, \cdots, w_r)$ over $k_0(y)$ must be trivial. In fact, applying D to (1), we get:

$$0 = \sum_{i=1}^{r} (T - \sum_{\mu} w_{i\mu} U_\mu)^{-1} \sum_{\mu} D w_{i\mu} U_\mu;$$

as the w_i are all distinct, this cannot be an identity in $T, U_1, \cdots, U_m$ unless all the $Dw_{i\mu}$ are 0.

PROPOSITION 7. *Notations being as defined above, we have $k'(y) = k'(u)$ provided the s_i are all distinct and satisfy the following condition:*

(S) *The set of points $\bar{s}_i = \Phi_0(s_i)$ on $\boldsymbol{G}$ is not mapped onto itself by any right-translation.*

The cycle $\sum(w_i)$ is the image of the cycle $\sum(s_i)$ by the mapping

$x \to xu$ of V into W; it is therefore rational over $k'(u)$. By the main theorem on symmetric functions (VA, no. 7, Th. 1), this implies that y is rational over $k'(u)$, i.e. that $k'(y) \subset k'(u)$. On the other hand, the lemma shows that the w_i are separably algebraic over $k''(y)$; as we have $u = s_i^{-1} w_i$ by Prop. 5 of § II, no. 5, u is therefore separably algebraic over $k''(y)$, hence also over $k'(y)$. Let σ be any automorphism over $k'(y)$ of the algebraic closure of $k'(y)$; as it induces an isomorphism of $k'(u)$ onto $k'(u^\sigma)$ over k', u^σ is generic on W over k', so that $s_i u^\sigma$ is defined by Prop. 5. This gives $(s_i u)^\sigma = s_i^\sigma u^\sigma$, i.e. $w_i^\sigma = s_i^\sigma u^\sigma$. But the decomposition of the homogeneous polynomial $y(T, U)$ into linear factors is uniquely determined; applying σ to (1), we see thus that the w_i^σ must be the same as the w_i except for a permutation, i.e. that there is a permutation $i \to \sigma(i)$ such that $w_i^\sigma = w_{\sigma(i)}$. This can be written as $s_i^\sigma u^\sigma = s_{\sigma(i)} u$; as the s_i^σ are the same as the s_i except for a permutation, we can write them as $s_i^\sigma = s_{\tau(i)}$, where $i \to \tau(i)$ is a permutation. Then we have $\Phi(s_{\tau(i)} u^\sigma) = \Phi(s_{\sigma(i)} u)$, which can be written as $\bar{s}_{\tau(i)} \Phi(u^\sigma) = \bar{s}_{\sigma(i)} \bar{u}$, i.e. $\Phi(u^\sigma) = \bar{s}_{\tau(i)}^{-1} \bar{s}_{\sigma(i)} \bar{u}$. As $\boldsymbol{G}$ acts faithfully on $\boldsymbol{S}$, the corollary of Prop. 5 shows that all the elements $\bar{s}_{\tau(i)}^{-1} \bar{s}_{\sigma(i)}$ of $\boldsymbol{G}$, for $1 \leqq i \leqq r$, must coincide; if $\bar{t}$ is their common value, we have $\bar{s}_{\sigma(i)} = \bar{s}_{\tau(i)} \bar{t}$, which shows that the right-translation $\bar{t}$ maps the set $\bar{s}_i$ onto itself. By (S), this implies that $\bar{t}$ is the neutral element of $\boldsymbol{G}$, so that $\Phi(u^\sigma) = \bar{u}$, and therefore $u^\sigma = u$. As u is separably algebraic over $k'(y)$, this shows that $k'(u) \subset k'(y)$.

8. Proposition 7 shows that we may write $y = f(u)$, where f is a birational correspondence, defined over k', between W and the locus Y of y over k' in affine space. If $k'[y]$ is the ring generated over k' by the coordinates of y, it is well-known that the integral closure of $k'[y]$ in $k'(y)$ is a finitely generated ring over k', i.e. that it can be written as $k'[y^*]$, where y^* is a point in a suitable affine space; call Y^* the locus of y^* over k' in that affine space. As we have $k'(y^*) = k'(y) = k'(u)$, we may write $y^* = f^*(u)$, f^* being a birational correspondence between W and Y^*, defined over k'. It is usual to say that Y^* is derived from Y by "normalization" over k'. By Prop. 14 of the Appendix, since k'' is separably algebraic over k', $k''[y^*]$ is integrally closed in $k''(y^*)$.

PROPOSITION 8. *With the notations explained above, y^* and $\bar{u}$ are corresponding generic points over K'' on Y^* and $\boldsymbol{S}$ in a birational correspondence between Y^* and $\boldsymbol{S}$ which maps Y^* biregularly onto the K''-open set $\Omega = \bigcap_i \bar{s}_i^{-1} \Phi(W)$ on $\boldsymbol{S}$.*

In the first place, we prove that the coordinates $w_{i\mu}$ of the w_i are all in $k''[y^*]$; as they are in $k''(y)$ because of the relations $w_i = s_i u$ and $k'(u) = k'(y)$, it will be enough to show that they are integral over the ring $k''[y]$, or in other words (e.g. by F-App. II, Prop. 6) that they are everywhere finite on W. In fact, let π be any place of $k''(y)$ such that $y(\pi)$ is finite. Take r independent variables $\lambda_1, \cdots, \lambda_r$ over $k''(y)$, and extend π to a place π' of $k''(y, \lambda_1, \cdots, \lambda_r)$ at which every one of the r points $(\lambda_i, \lambda_i w_{i1}, \cdots, \lambda_i w_{im})$ is finite and $\neq (0, \cdots, 0)$. The relation (1), by which y was defined, can be written

$$\lambda_1 \cdots \lambda_r y(T, U) = \prod_{i=1}^{r} (\lambda_i T - \sum_{\mu} (\lambda_i w_{i\mu}) U_\mu).$$

Taking the values of both sides at π', we see that the right-hand side does not become identically 0 at that place; as $y(\pi)$ is finite, this implies that no λ_i can become 0 at π'; but then $w_{i\mu}(\pi)$ can be written as $(\lambda_i w_{i\mu})(\pi')/\lambda_i(\pi')$ and is finite. This proves the assertion about the $w_{i\mu}$.

We have thus shown that the mappings $y^* \to w_i$ of Y^* into W are everywhere defined on Y^*; as we have $\bar{u} = \bar{s}_i^{-1} \Phi(w_i)$, this implies that $y^* \to \bar{u}$ is everywhere defined and maps Y^* into the set Ω defined in Prop. 8. Conversely, the definition of y can be written

$$y(T, U) = \prod_{i=1}^{r} (T - \sum_{\mu} \Psi_\mu(\bar{s}_i \bar{u}) U_\mu)$$

if we call $\Psi_\mu(\bar{u})$ the coordinates of $\Psi(\bar{u})$. As Ψ is everywhere defined on $\Phi(W)$, this shows that the mapping $\bar{u} \to y$ is defined at every point of the set Ω. As $k'[y^*]$ is the integral closure of $k'[y]$ in $k'(y)$, it is therefore contained in the integral closure of the specialization-ring of every point of Ω on $\boldsymbol{S}$. But we have assumed that W and consequently $\boldsymbol{S}$ are normal, i.e. that the specialization-ring of every point of $\boldsymbol{S}$ (over any field of definition for $\boldsymbol{S}$) is integrally closed. This proves that $\bar{u} \to y^*$ is everywhere defined on the set Ω. In view of what we have proved above, Ω is therefore the set of points of $\boldsymbol{S}$ where this mapping is defined, and is K''-open by Prop. 8 of the Appendix; more precisely, it is K'-open if K' is the compositum of K and k'. This completes the proof.

9. Denote now by S any cycle $\sum_i (s_i)$ on V, *rational over the ground-field* k, consisting of distinct points s_i and satisfying condition (S). From such a set S, and taking $k' = k$, we can derive as above a point y, which we now write as y_S, and furthermore a point $y_S{}^*$ such that $k[y_S{}^*]$ is the integral

closure of $k[y_S]$ in $k(y_S)$; as above, we call Y_S^* the locus of y_S^* over k; we write Ω_S for the open subset of $\boldsymbol{S}$ denoted by Ω in Prop. 8. If we allow S to run through any finite set of cycles with the properties stated above, then all the varieties Y_S^* will be birationally equivalent to W and to each other, and we can take the points y_S^* to be corresponding generic points of these varieties over k. It is then an immediate consequence of Prop. 8 that the affine varieties Y_S^* (with empty "frontiers"), and the birational correspondences between them for which the y_S^* are corresponding generic points of the Y_S^* over k, determine an abstract variety $\boldsymbol{S}'$, and that this is biregularly equivalent over a suitable field (as a matter of fact, over K itself) with the union of the open sets Ω_S on $\boldsymbol{S}$. In order to prove that $\boldsymbol{S}'$ will be biregularly equivalent to $\boldsymbol{S}$ itself for a suitable choice of the cycles S, it is therefore enough, in view of the well-known "compactoid" property of open sets in the Zariski topology, to show that the family of all open sets Ω_S is a covering of $\boldsymbol{S}$. In other words, we have to prove the following:

PROPOSITION 9. *Given any point $\bar{a}$ on $\boldsymbol{S}$, there is a cycle $S = \sum_i (s_i)$ on V, rational over k, consisting of distinct points s_i and satisfying condition* (S), *and such that $\bar{s}_i\bar{a} \in \Phi(W)$ for all i.*

Assume that $\bar{a}$ has a representative a_α on S_α; take x generic over $K(\bar{a}) = K(a_\alpha)$ on V, and put $u = (xt_\alpha^{-1})a_\alpha$, this being defined because W is a chunk. If we put, as usual, $\bar{x} = \Phi_0(x)$ and $\bar{u} = \Phi(u)$, we have then $\bar{u} = \bar{x}\bar{a}$, so that $u = \Psi(\bar{x}\bar{a})$. As the mapping $x \to \bar{x}\bar{a}$ is everywhere defined on V, this shows that the mapping $x \to u$ of V into W is defined at the points s of V such that $\bar{s}\bar{a} \in \Phi(W)$, and at those points only. Let F be the closed subset of V where the mapping $x \to u$ is not defined; by Prop. 12 of the Appendix, there is a maximal k-closed subset F_0 of V contained in F; then an algebraic point of V over k is in F if and only if it is in F_0. Call F_1 the union of the conjugates over k of all the components of F_0; this is a k-closed set on V, and its definition shows that the cycle S on V will satisfy the last one of the conditions stated in Prop. 9 if and only if it lies in $V - F_1$.

Now assume first that the field k is infinite. Applying Prop. 13 of the Appendix to the variety $V' = V - F_1$, and to the empty subset of $V' \times V'$, we obtain a separably algebraic point s_1 over k on V'; call $s_1, \cdots, s_d$ all the distinct conjugates of s_1 over k; if this set satisfies condition (S), which will be the case in particular if $d = 1$, then it solves our problem. Suppose that this is not so, and therefore that $d > 1$. For any $r > d$, let $s_{d+1}, \cdots, s_r$ be any set of $r - d$ points on $V - F_1$, distinct from one another and from $s_1, \cdots, s_d$; put $S' = \{\bar{s}_1, \cdots, \bar{s}_d\}$ and $S'' = \{\bar{s}_{d+1}, \cdots, \bar{s}_r\}$. If the set

$S' \cup S''$ is mapped into itself by a right-translation τ other than the identity, one of the following circumstances must occur: (i) τ maps each one of the sets S', S'' onto itself; then τ is of the form $s'^{-1}t'$, with s', t' in S', and there must be two elements s'', t'' of S'' such that $t'' = s''\tau$; (ii) τ maps S' into S''; as $d > 1$, we can choose two distinct elements s', t' in S', and then $s'' = s'\tau$, $t'' = t'\tau$ are in S'', so that we have $t'' = (t's'^{-1})s''$; (iii) τ maps some $s' \in S'$ onto some $s'' \in S''$ and some $t' \in S'$ onto some $t_1' \in S'$; then $s'' = s't'^{-1}t_1'$. Thus, in order to satisfy the requirements of Prop. 9, it is enough to take as $s_{d+1}, \cdots, s_r$ the conjugates over k of a point $s = s_{d+1}$ of $V - F_1$, separably algebraic over k, satisfying the following conditions: (a) no $\bar{s}_l$, for $d+1 \leqq l \leqq r$, coincides with any of the points $\bar{s}_i$ or $\bar{s}_i\bar{s}_j^{-1}\bar{s}_h$ for $1 \leqq i, j, h \leqq d$; (b) no pair of distinct conjugates of s over k lies on the graph of any of the birational correspondences $x \to \Psi(\bar{x}\bar{s}_i^{-1}\bar{s}_j)$, $x \to \Psi(\bar{s}_i\bar{s}_j^{-1}\bar{x})$ for $1 \leqq i, j \leqq d$. As to (a), it will be satisfied provided we take s on $V - F_2$, where F_2 is the union of F_1, of the set $s_1, \cdots, s_d$, and of the set of all conjugates over k of those algebraic points on V whose image on $\boldsymbol{G}$ coincides with one of the points $\bar{s}_i\bar{s}_j^{-1}\bar{s}_h$. Then our result follows at once by applying Prop. 13 of the Appendix to the variety $V - F_2$ and to the union of the graphs of the birational correspondences in (b).

If k is finite, we have to proceed differently. Take any algebraic point s_1 over k on $V - F_1$; call $s_1, \cdots, s_d$ its distinct conjugates over k; if this set satisfies condition (S), it solves our problem. If not, we use a result of Lang-Weil (this JOURNAL, vol. 76 (1954), p. 819) which says that, if l is sufficiently large, there must be a point s on $V - F_1$ which is rational over the (unique) extension of k of degree l. We take l prime and $> d$. If s is rational over k, the cycle (s) solves our problem; if not, it is of degree l over k; call $s_{d+1}, \cdots, s_{d+l}$ its distinct conjugates over k; they are distinct from $s_1, \cdots, s_d$, since the latter are of degree d over k. The set $s_{d+1}, \cdots, s_{d+l}$ may solve our problem. If it does not, the group $\mathfrak{g}$ of right-translations mapping the set $\{\bar{s}_{d+1}, \cdots, \bar{s}_{d+l}\}$ onto itself is of order $\nu > 1$; as that set must be the union of cosets with respect to $\mathfrak{g}$, ν must divide l, and so $\mathfrak{g}$ is cyclic of order l; call τ a generator of $\mathfrak{g}$. Let τ' be a right-translation mapping onto itself the set $\{\bar{s}_1, \cdots, \bar{s}_{d+l}\}$. If τ' is not the identity and maps some element of the set $\{\bar{s}_{d+1}, \cdots, \bar{s}_{d+l}\}$ into an element of the same set, it must be of the form τ^i, and therefore of order l; but this cannot be, since $d + l$ is not a multiple of l. Therefore τ' must map the set $\{\bar{s}_{d+1}, \cdots, \bar{s}_{d+l}\}$ into the set $\{\bar{s}_1, \cdots, \bar{s}_d\}$. As $d < l$, this is also impossible. Therefore the set $s_1, \cdots, s_{d+l}$ solves our problem.

This completes the proof of the results announced at the beginning of

no. 7. Writing now G, S instead of $\boldsymbol{G}'$, $\boldsymbol{S}'$, we may restate them in a somewhat more complete form as follows:

THEOREM. (i) *To every pre-group V, defined over a field k, there is a birationally equivalent group G, also defined over k; this is uniquely determined up to an isomorphism.*

(ii) *To every pre-homogeneous space W with respect to V, defined over k, there is a birationally equivalent homogeneous space with respect to G, also defined over k; this is uniquely determined up to an isomorphism.*

(iii) *Let W be a pre-transformation space with respect to V, defined over k; let a be a point of W such that W is normal at a and that, if x is generic over $k(a)$ on V, xa and $x^{-1}(xa)$ are defined. Then there is a transformation-space S with respect to G, birationally equivalent to W over k in such a way that the birational correspondence between them is biregular at a; S may be taken everywhere normal, and it may be taken to be non-singular if a is simple on W. Moreover, S is uniquely determined up to a birational correspondence which is biregular at every point of the form $\bar{s}\bar{a}$, where $\bar{a}$ is the point corresponding to a on S and $\bar{s}$ is any point of G.*

Except for the statements about unicity, all this has been proved above. As to unicity, the statements in (i) and (ii) are special cases of the statement in (iii); and the latter is an immediate consequence of the fact that the operations of G are everywhere biregular mappings of S onto S.

Appendix.

If X is any cycle, we denote by $|X|$ the *support* of X, i.e. the closed set which is the set-theoretic union of the components of X.

PROPOSITION 1. *Let $k(x)$ be a regular extension of a field k, and $k(x,y)$ a regular extension of $k(x)$. Then $k(x,y)$ is a regular extension of k.*

This is an immediate consequence of F-I$_7$, Th. 5.

PROPOSITION 2. *Let $k(x)$ be a regular extension of a field k; let K be an overfield of k, linearly disjoint from $k(x)$ over k; let k' be the algebraic closure of k in K. Then $k'(x)$ is the algebraic closure of $k(x)$ in $K(x)$.*

Let y be an element of $K(x)$, algebraic over $k(x)$; we may take x to be

a generic point over K of a variety V, defined over k, in an affine space; and then we may write $y = F(x)$, where F is a function on V, defined over K; call Γ the graph of F. As y is algebraic over $k(x)$, there is a polynomial $P \in k[X, Y]$ such that $P(x, Y) \neq 0$ and $P(x, y) = 0$; then P induces on the product $V \times D$ of V and of the affine space D of dimension 1 a function which is not 0 on $V \times D$ and is 0 on Γ. As Γ has the same dimension as V, it must be a component of the divisor (P) of P, and is therefore algebraic over k. The smallest field of definition of Γ containing k must then be contained in k', so that F is defined over k'; this implies that y is in $k'(x)$.

COROLLARY. *If K is primary over k, $K(x)$ is primary over $k(x)$.*

In fact, the assumption means that k' is purely inseparable over k; this implies that $k'(x)$ is purely inseparable over $k(x)$.

PROPOSITION 3. *Let $k(x)$ be a finitely generated extension of a field k; then every field K such that $k \subset K \subset k(x)$ is finitely generated over k.*

Let $t = (t_1, \cdots, t_n)$ be a maximal set of algebraically independent elements of K over k; then K is algebraic over $k(t)$. Replacing k by $k(t)$, we see that it is enough to prove our proposition in the case when K is algebraic over k. This being assumed, call k' the smallest field of definition containing k for the locus of x over the algebraic closure $\bar{k}$ of k; then k' is a finite algebraic extension of k and is algebraically closed in $k'(x)$ since $k'(x)$ is regular over k'. But then k' is the algebraic closure of k in $k'(x)$ and therefore contains the algebraic closure of k in $k(x)$, so that K is contained in k'.

COROLLARY. *If $k(x)$ is regular over k, so is K.*

PROPOSITION 4. *Let t be a point, k a field, and let $t_1, \cdots, t_N$ be N independent generic specializations of t over k. Let x be a point of dimension $d < N$ over k and such that $k(x)$, $k(t)$ are linearly disjoint over k. Then there is an α such that t_α is a generic specialization of t over $k(x)$.*

Call n the dimension of $k(t)$ over k. By F-I$_6$, Th. 3, every t_α is a specialization of t over $k(x)$; if none is generic, every t_α must have over $k(x)$ a dimension $\leqq n-1$; but then $(x, t_1, \cdots, t_N)$ has over k a dimension $\leqq d + N(n-1) < Nn$, which is impossible, since $(t_1, \cdots, t_N)$ has the dimension Nn over k.

PROPOSITION 5. *Let V be a variety, defined over a field k; let K be an overfield of k and x a point of V. Let A and A' be the prime rational cycles,*

over k and over K respectively, with the generic point x. Then A is the same as A' if and only if K and $k(x)$ are linearly disjoint over k.

We may replace V by any representative of V on which x has a representative, so that it is enough to prove our result for cycles in the affine n-space. For A to be the same as A', it is at any rate necessary that they should have the same dimension, so that K and $k(x)$ must be independent over k; assume from now on that this is so. Among the coordinates of x, let $(x_1, \cdots, x_r)$ be a maximal set of independent variables over k and therefore also over K; write y for the point $(x_1, \cdots, x_r)$ and z for $(x_{r+1}, \cdots, x_n)$. By F-VII$_6$, Th. 12, $A = A'$ if and only if $A \cdot (y \times S^{n-r})$ is the same as $A' \cdot (y \times S^{n-r})$; by F-VI$_3$, Th. 12, this is so if and only if z has the same complete set of conjugates over $K(y)$ as over $k(y)$, and therefore, by F-I$_4$, Prop. 12 and F-I$_2$, Prop. 6, if and only if $K(y)$ and $k(y,z) = k(x)$ are linearly disjoint over $k(y)$. The latter condition means that there is no relation $\sum_i u_i \Phi_i(y) = 0$ in which the u_i are linearly independent elements of $k(x)$ over $k(y)$ and the $\Phi_i(y)$ are in $K[y]$ and not all 0. Assume that there is such a relation; we may write $\Phi_i(y) = \sum_j P_{ij}(y)\xi_j$, where the ξ_j are linearly independent elements of K over k and the $P_{ij}(y)$ are in $k[y]$ and not all 0. Then we have $\sum_j v_j \xi_j = 0$ with $v_j = \sum_i u_i P_{ij}(y)$; as the v_j are in $k(x)$ and not all 0 because of the assumptions on the u_i and $P_{ij}(y)$, this shows that, when that is so, K and $k(x)$ are not linearly disjoint over k. Conversely, assume that there is a relation $\sum_j v_j \xi_j = 0$ in which the ξ_j are linearly independent elements of K over k and the v_j are in $k(x)$ and not all 0; as the ξ_j are then also linearly independent elements of $K(y)$ over $k(y)$, this implies that $K(y)$ and $k(x)$ are not linearly disjoint over $k(y)$.

COROLLARY. *Let V be a variety, defined over a field k. Let A be a prime rational cycle on V over an overfield K of k. Then, if K' is any field such that $k \subset K' \subset K$ over which A is rational, A is prime rational over K'; of all such fields K', there is one smallest one K_0; and an automorphism σ of K over k transforms A into itself if and only if it induces the identity on K_0.*

As in the proof of Prop. 5, it is enough to consider cycles in an affine space. Assume that A is prime rational over K and rational over $K' \subset K$, and write it as $A = \sum_i n_i A_i$, where the A_i are distinct prime rational cycles over K'. Let Z be a component of A_1; it is algebraic over K', and so every conjugate of Z over K is a fortiori such over K', so that every component of

A is a component of A_1; therefore we must have $A = n_1 A_1$. By F-I$_8$, Prop. 26, the coefficient of Z in A is at most equal to its coefficient in A_1; therefore we have $A = A_1$. That being so, it follows from Prop. 5 and from F-I$_6$, Th. 3 and F-I$_7$, Lemma 2, that there is a smallest field K_0 with the properties stated in our corollary; in fact, if x is a generic point of A over K, and if $\mathfrak{P}$ is the prime ideal in $K[X]$ consisting of all polynomials in $K[X]$ which are 0 at x, K_0 is the smallest subfield of K such that $\mathfrak{P}$ has a set of generators in $K_0[X]$. As $\mathfrak{P}$ is also the ideal in $K[X]$ whose set of zeros is the support $|A|$ of A, the last assertion follows from F-I$_7$, Lemma 2.

PROPOSITION 6. *Let V be a variety, defined over a field k, and A a cycle on V; assume either that A is a divisor on V or that the coefficients in A of all the components of A are $\not\equiv 0 \bmod p$, p being the characteristic. Then, of all the overfields of k over which A is rational, there is one smallest one k_0, k_0 is finitely generated over k; and an isomorphism σ of k_0 over k onto some extension of k leaves A invariant if and only if it leaves every element of k_0 invariant.*

Except for the last statement, this result is due to Chow. Let A be any cycle on V; for every representative V_α of V, call A_α the sum of the terms in the reduced expression for A which pertain to components with representatives in V_α; then A is rational over an overfield K of k if and only if every A_α is rational over K; and an isomorphism of K which leaves A invariant must leave all the A_α invariant. Therefore it is enough to deal with cycles on an affine variety V. For such a cycle A, put $A = \sum_n n A_n$, where A_n is the sum of the terms with the coefficient n in the reduced expression for A; then A is rational if and only if every cycle nA_n is rational; and an isomorphism which leaves A invariant must leave all the A_n invariant. Finally, if $n = p^\nu n'$ with n' prime to p, nA is rational if and only if $p^\nu A$ is rational. Therefore it will be enough to deal with the following two cases: (i) A is a cycle in affine space, consisting of a sum of distinct components; (ii) A is a divisor on an affine variety V and of the form $A = qA_0$, where q is a power of p and A_0 is a sum of distinct components.

(i) Let $\mathfrak{A}$ be the ideal of all polynomials (with coefficients in the universal domain) which are 0 on the support $|A|$ of A; this is the intersection of the prime ideals determined similarly by the components of A. The first assertion in our proposition will then be a consequence of F-I$_7$, Lemma 2, if we prove that A is rational over a field K if and only if $\mathfrak{A}$ has a set of generators in $K[X]$, i. e. if it is the extension to the universal domain

of the ideal $\mathfrak{A} \cap K[X]$; the second assertion in our proposition also follows from the same lemma, provided one observes that, if k_0 is the smallest field such that $\mathfrak{A}$ has a set of generators in $k_0[X]$, an isomorphism which leaves A invariant must map k_0 onto k_0, i.e. it must induce an automorphism in k_0, so that the lemma in question is applicable.

If $\mathfrak{A}$ has a set of generators (P_ν) in $K[X]$, the support $|A|$ of A is the set of zeros of the P_ν and is therefore K-closed. On the other hand, $|A|$ must also be K-closed if A is rational over K. In order to prove the equivalence of those two properties, one may then begin by assuming that $|A|$ is K-closed. Consider first the case in which all the components of A are the conjugates of one of them, say Z, over K; let x be a generic point of Z over K; then A is rational over K if and only if $K(x)$ is separable over K. Put $K' = K^{p^{-\infty}}$, this being the smallest "perfect" field containing K. Put:

$$\mathfrak{P} = \mathfrak{A} \cap K[X], \qquad \mathfrak{P}' = \mathfrak{A} \cap K'[X],$$

and call $\mathfrak{Q}'$ the extension of $\mathfrak{P}$ to $K'[X]$. By F-IV$_2$, Th. 4, and F-II$_1$, Prop. 3, $\mathfrak{P}$ and $\mathfrak{P}'$ consist of the polynomials, in $K[X]$ and in $K'[X]$ respectively, which are 0 at x; they are prime ideals; moreover, if $P' \in \mathfrak{P}'$, some power P'^n of P' is in $\mathfrak{P}'$ and hence in $\mathfrak{Q}'$; as $\mathfrak{Q}' \subset \mathfrak{P}'$, this implies that $\mathfrak{Q}'$ is primary and belongs to the prime ideal $\mathfrak{P}'$. By F-I$_6$, Th. 3, and F-I$_7$, Prop. 19, we see that $\mathfrak{P}' = \mathfrak{Q}'$ if and only if $K(x)$ is separable over K, and therefore, as we have shown, if and only if A is rational over K. But, if $\mathfrak{A}$ is the extension of $\mathfrak{P}$ to the universal domain, $\mathfrak{P}'$ must a fortiori be the extension of $\mathfrak{P}$ to $K'[X]$. Conversely, if $\mathfrak{Q}' = \mathfrak{P}'$, the extension of $\mathfrak{P}$ to the universal domain is the same as that of $\mathfrak{P}'$; but it is well-known and easily verified that the latter must be a "radical" ideal, i.e. one consisting of all the polynomials which are 0 on a closed set; then one sees at once that it must be the same as $\mathfrak{A}$. This completes the proof in the special case we were considering.

Now assume that $|A|$ is any K-closed set; then we can write A as the sum of cycles A_i such that the components of each A_i are mutually conjugate over K, and $\mathfrak{A}$ is the intersection of the ideals $\mathfrak{A}_i$ similarly determined by the A_i. Put:

$$\mathfrak{P}_i = \mathfrak{A}_i \cap K[X], \qquad \mathfrak{P}_i' = \mathfrak{A}_i \cap K'[X],$$

and call $\mathfrak{Q}_i'$ the extension of $\mathfrak{P}_i$ to $K'[X]$. If A is rational over K, all the A_i must be so, so that, as shown above, the $\mathfrak{A}_i$ must be the extensions of the $\mathfrak{P}_i$ to the universal domain. It is then easily seen that $\mathfrak{A}$ is the extension of the intersection of the $\mathfrak{P}_i$, i.e. of $\mathfrak{A} \cap K[X]$. Assume, on the other hand, that A is not rational over K; then we have $\mathfrak{Q}_i' \neq \mathfrak{P}_i'$ for at least one i; from

the unicity of the decomposition of an ideal into an intersection of primary ideals, it follows then that the intersection of the $\mathfrak{Q}_i'$, which is the extension of $\mathfrak{A} \cap K[X]$ to $K'[X]$, cannot be the same as the intersection of the $\mathfrak{P}_i'$, which is $\mathfrak{A} \cap K'[X]$. A fortiori, $\mathfrak{A}$ cannot then be the extension of $\mathfrak{A} \cap K[X]$ to the universal domain. This completes the proof for case (i).

(ii) Let V be a variety, defined over k, in an affine space; let A_0 be a divisor on V and the sum of distinct components; let q be a power of the characteristic $p \neq 0$; put $A = qA_0$. If P is any polynomial which is not 0 on V, denote by $(P)_V$ the divisor of the function induced by P on V. Call $\mathfrak{A}$ the ideal of all the polynomials P, with coefficients in the universal domain, such that either $P = 0$ on V or $(P)_V \succ A$. If A is rational over an overfield K of k, $\mathfrak{A}$ is then the extension of $\mathfrak{A} \cap K[X]$ to the universal domain, as follows at once from F-VIII$_3$, Th. 10. Conversely, assume that $\mathfrak{A}$ is the extension of $\mathfrak{A} \cap K[X]$ to the universal domain; we will prove that A is then rational over K; our proposition will then follow from this as in case (i). As a polynomial P is 0 on $|A|$ if and only if some power P^n of P is in $\mathfrak{A}$, our assumption on A implies that A is K-closed, and therefore that A_0 is rational over $K' = K^{p^{-\infty}}$. Let Z be a component of A. As well-known, there is a polynomial P such that $(P)_V = A_0 + B$, where B has no component in common with A_0; write P as $P = \sum_i \xi_i P_i$, where the ξ_i are linearly independent over K' and the P_i are in $K'[X]$; by F-VIII$_3$, Th. 10, we have $(P_i)_V \succ A_0$ for all i; and Z must have the coefficient 1 in at least one of the P_i, since otherwise it would occur in B; if we call that polynomial P', P' is then in $K'[X]$, Z has the coefficient 1 in $(P')_V$, and we have $(P')_V \succ A_0$. But then P'^q is in $\mathfrak{A}$, and therefore, by hypothesis, may be written as $\sum_j \eta_j Q_j$, where the Q_j are in $\mathfrak{A} \cap K[X]$. The latter fact implies that Z has at least the coefficient q in all the $(Q_j)_V$; as it has the coefficient q in P'^q, it must have the coefficient q in one at least of the divisors $(Q_j)_V$; as these divisors are rational over K, this implies that, if A_1 is the sum of Z and its conjugates over K, qA_1 is rational over K. As this is so for every component Z of A, A is therefore rational over K.

PROPOSITION 7. *Let U, V be two varieties, defined over a field k; let F be a k-closed subset of $U \times V$. Then the set A of the points a on U such that $a \times V \subset F$ is k-closed.*

Let $W_1, \cdots, W_m$ be those components of F which have the "projection" V on V (in the sense of F-IV$_3$, F-VII$_3$); if v is a generic point of V over k, W_i has a generic point over k of the form (u_i, v); and $a \in A$ if and only if,

for v' generic over $k(a)$ on V, (a, v') is a specialization of some (u_i, v) over $\bar{k}$. Let V_1 be any representative of the abstract variety V; let v_1 be the representative of v on V_1; the ambient affine space for V_1 being embedded in a projective space, let V_0 be the locus of v_1 over k in that projective space. Let F_0 be the union of the loci of the points (u_i, v_1) over $\bar{k}$ in $U \times V_0$; F_0 is k-closed on $U \times V_0$. Then A is the set of the points a on U such that $F_0 \cap (a \times V_0)$ has a component of dimension $\geqq \dim(V_0)$. As V_0 is complete, our conclusion is now contained in Lemma 7 of my paper in *Math. Ann.*, vol. 128 (1954), p. 104.

PROPOSITION 8. *Let ϕ be a mapping of a variety U into a variety V; let k be a field of definition for U, V and ϕ. Then the set of points of U where ϕ is defined is k-open.*

(i) Assume first that U is an affine variety and V is the affine space of dimension 1. Let x be a generic point of U over k; put $y = \phi(x)$. Let $\mathfrak{A}$ be the set of all polynomials P in $k[X]$ such that $P(x)y$ is in $k[x]$; this is an ideal in $k[X]$, containing the ideal $\mathfrak{P}$ of those polynomials which are 0 at x and therefore on V. Since y may be written as $Q(x)/P(x)$, with P, Q in $k[X]$ and $P(x) \neq 0$, we have $\mathfrak{A} \neq \mathfrak{P}$. As the points where ϕ is not defined are the zeros of $\mathfrak{A}$, the set of such points is k-closed.

(ii) Take V as in (i), and assume that U is an abstract variety, with the representatives U_α, on each of which a "frontier" F_α (i.e. a k-closed set) is given, according to the definitions in F-VII$_1$. Call F_α' the k-closed subset of U_α where ϕ is not defined; the set F of the points of U where ϕ is not defined is then the union of the images of the sets $F_\alpha' \cap (U_\alpha - F_\alpha)$ by the canonical birational mappings of the U_α into U. It is easily seen that F must be k-closed provided the following assertion is true: if x is a point of U with a representative x_α on some U_α which is a generic point over $\bar{k}$ of a component of F_α', then every specialization x' of x over k is in F. In fact, let β be such that x' has a representative x_β' on U_β; then x must also have a representative x_β on U_β, and, from the biregularity of the correspondence between U_α, U_β at (x_α, x_β), it follows that x_β must be in F_β'; as x_β' is a specialization of x_β over k, and as F_β' is k-closed, x_β' must then be in F_β', so that x' is in F. This proves our result for this case.

It follows trivially from this that our result remains true when U is an abstract variety and V is an affine space or more generally an affine variety.

(iii) Let U be an abstract variety and let V be a k-open subset of an affine variety V_1; let V_0 be the projective variety whose part "at finite dis-

the unicity of the decomposition of an ideal into an intersection of primary ideals, it follows then that the intersection of the $\mathfrak{Q}_i'$, which is the extension of $\mathfrak{A} \cap K[X]$ to $K'[X]$, cannot be the same as the intersection of the $\mathfrak{P}_i'$, which is $\mathfrak{A} \cap K'[X]$. A fortiori, $\mathfrak{A}$ cannot then be the extension of $\mathfrak{A} \cap K[X]$ to the universal domain. This completes the proof for case (i).

(ii) Let V be a variety, defined over k, in an affine space; let A_0 be a divisor on V and the sum of distinct components; let q be a power of the characteristic $p \neq 0$; put $A = qA_0$. If P is any polynomial which is not 0 on V, denote by $(P)_V$ the divisor of the function induced by P on V. Call $\mathfrak{A}$ the ideal of all the polynomials P, with coefficients in the universal domain, such that either $P = 0$ on V or $(P)_V \succ A$. If A is rational over an overfield K of k, $\mathfrak{A}$ is then the extension of $\mathfrak{A} \cap K[X]$ to the universal domain, as follows at once from F-VIII$_3$, Th. 10. Conversely, assume that $\mathfrak{A}$ is the extension of $\mathfrak{A} \cap K[X]$ to the universal domain; we will prove that A is then rational over K; our proposition will then follow from this as in case (i). As a polynomial P is 0 on $|A|$ if and only if some power P^n of P is in $\mathfrak{A}$, our assumption on A implies that A is K-closed, and therefore that A_0 is rational over $K' = K^{p^{-\infty}}$. Let Z be a component of A. As well-known, there is a polynomial P such that $(P)_V = A_0 + B$, where B has no component in common with A_0; write P as $P = \sum_i \xi_i P_i$, where the ξ_i are linearly independent over K' and the P_i are in $K'[X]$; by F-VIII$_3$, Th. 10, we have $(P_i)_V \succ A_0$ for all i; and Z must have the coefficient 1 in at least one of the P_i, since otherwise it would occur in B; if we call that polynomial P', P' is then in $K'[X]$, Z has the coefficient 1 in $(P')_V$, and we have $(P')_V \succ A_0$. But then P'^q is in $\mathfrak{A}$, and therefore, by hypothesis, may be written as $\sum_j \eta_j Q_j$, where the Q_j are in $\mathfrak{A} \cap K[X]$. The latter fact implies that Z has at least the coefficient q in all the $(Q_j)_V$; as it has the coefficient q in P'^q, it must have the coefficient q in one at least of the divisors $(Q_j)_V$; as these divisors are rational over K, this implies that, if A_1 is the sum of Z and its conjugates over K, qA_1 is rational over K. As this is so for every component Z of A, A is therefore rational over K.

PROPOSITION 7. *Let U, V be two varieties, defined over a field k; let F be a k-closed subset of $U \times V$. Then the set A of the points a on U such that $a \times V \subset F$ is k-closed.*

Let $W_1, \cdots, W_m$ be those components of F which have the "projection" V on V (in the sense of F-IV$_3$, F-VII$_3$); if v is a generic point of V over k, W_i has a generic point over k of the form (u_i, v); and $a \in A$ if and only if,

for v' generic over $k(a)$ on V, (a, v') is a specialization of some (u_i, v) over $\bar{k}$. Let V_1 be any representative of the abstract variety V; let v_1 be the representative of v on V_1; the ambient affine space for V_1 being embedded in a projective space, let V_0 be the locus of v_1 over k in that projective space. Let F_0 be the union of the loci of the points (u_i, v_1) over $\bar{k}$ in $U \times V_0$; F_0 is k-closed on $U \times V_0$. Then A is the set of the points a on U such that $F_0 \cap (a \times V_0)$ has a component of dimension $\geqq \dim(V_0)$. As V_0 is complete, our conclusion is now contained in Lemma 7 of my paper in *Math. Ann.*, vol. 128 (1954), p. 104.

PROPOSITION 8. *Let ϕ be a mapping of a variety U into a variety V; let k be a field of definition for U, V and ϕ. Then the set of points of U where ϕ is defined is k-open.*

(i) Assume first that U is an affine variety and V is the affine space of dimension 1. Let x be a generic point of U over k; put $y = \phi(x)$. Let $\mathfrak{A}$ be the set of all polynomials P in $k[X]$ such that $P(x)y$ is in $k[x]$; this is an ideal in $k[X]$, containing the ideal $\mathfrak{P}$ of those polynomials which are 0 at x and therefore on V. Since y may be written as $Q(x)/P(x)$, with P, Q in $k[X]$ and $P(x) \neq 0$, we have $\mathfrak{A} \neq \mathfrak{P}$. As the points where ϕ is not defined are the zeros of $\mathfrak{A}$, the set of such points is k-closed.

(ii) Take V as in (i), and assume that U is an abstract variety, with the representatives U_α, on each of which a "frontier" F_α (i.e. a k-closed set) is given, according to the definitions in F-VII$_1$. Call F_α' the k-closed subset of U_α where ϕ is not defined; the set F of the points of U where ϕ is not defined is then the union of the images of the sets $F_\alpha' \cap (U_\alpha - F_\alpha)$ by the canonical birational mappings of the U_α into U. It is easily seen that F must be k-closed provided the following assertion is true: if x is a point of U with a representative x_α on some U_α which is a generic point over $\bar{k}$ of a component of F_α', then every specialization x' of x over k is in F. In fact, let β be such that x' has a representative x_β' on U_β; then x must also have a representative x_β on U_β, and, from the biregularity of the correspondence between U_α, U_β at (x_α, x_β), it follows that x_β must be in F_β'; as x_β' is a specialization of x_β over k, and as F_β' is k-closed, x_β' must then be in F_β', so that x' is in F. This proves our result for this case.

It follows trivially from this that our result remains true when U is an abstract variety and V is an affine space or more generally an affine variety.

(iii) Let U be an abstract variety and let V be a k-open subset of an affine variety V_1; let V_0 be the projective variety whose part "at finite dis-

tance" is V_1; then $V_0 - V$ is a k-closed subset F_0 of V_0. Call Γ the graph of ϕ on $U \times V_0$; the set F of the points of U where ϕ, considered as a mapping of U into V, is not defined, is then the union of the set F_1 of the points of U where ϕ is not defined as a mapping of U into V_1 and of the set-theoretic projection of $\Gamma \cap (U \times F_0)$ on U. As V_0 is complete, the latter set coincides with the "projection" in the sense of F-IV$_3$ and F-VII$_3$ and is k-closed (e.g. by F-VII$_4$, Prop. 10 and 11); and F_1 is k-closed, as shown in (ii). Therefore F is k-closed.

(iv) Let U, V be arbitrary abstract varieties; let x be a generic point of U over k; let the V_α be those representatives of V on which $\phi(x)$ has a representative $\phi_\alpha(x)$, and let F_α be the "frontiers" on the V_α. Then ϕ is defined at a point of U if there is an α such that ϕ_α, considered as a mapping of U into $V_\alpha - F_\alpha$, is defined there. Therefore the set where ϕ is not defined is the intersection of the sets where the ϕ_α are not defined; as the latter sets are k-closed by (iii), this completes the proof.

COROLLARY 1. *Let V be an abstract variety, defined over k, with the representatives V_α. Then, for each α, the set Ω_α of the points of V which have a representative on V_α is k-open; and the canonical correspondence between V and V_α is an everywhere biregular mapping of Ω_α onto $V_\alpha - F_\alpha$ if F_α is the frontier for V_α.*

Let x be a generic point of V over k, and let x_α be its representative on V_α; if we put $x_\alpha = \phi_\alpha(x)$, ϕ_α is the "canonical correspondence" between V and V_α. Then Ω_α is the set of points where ϕ_α, considered as a mapping of V into $V_\alpha - F_\alpha$, is defined; it is k-open by Prop. 8. The rest is obvious.

COROLLARY 2. *Let V be an abstract variety, defined over a field k. Then there is a finite covering of V by k-open subsets of V, each of which is biregularly equivalent to an affine variety.*

Corollary 1 says that V has a covering by the k-open sets Ω_α, each of which is biregularly equivalent to the k-open subset $V_\alpha - F_\alpha$ of the affine variety V_α. It is therefore enough to prove our assertion for a k-open subset $V - F$ of an affine variety V defined over k. Let $\mathfrak{A}$ be the set of all polynomials in $k[X]$ which are 0 on F; it is an ideal in $k[X]$, and, as F is k-closed, it is the set of zeros of $\mathfrak{A}$. Let $P_1, \cdots, P_m$ be a set of generators for $\mathfrak{A}$; as $F \neq V$, they are not all 0 on V, and we may assume that $P_1, \cdots, P_r$ are not 0 on V while $P_{r+1}, \cdots, P_m$ are 0 on V, with $1 \leqq r \leqq m$. For $1 \leqq \rho \leqq r$, call Ω_ρ the k-open subset of V consisting of the points where P_ρ is not 0; the Ω_ρ are a covering of $V - F$. Let $x = (x_1, \cdots, x_n)$ be a generic

point of V over k; let V_ρ be the locus of the point

$$(x_1, \cdots, x_n, 1/P_\rho(x_1, \cdots, x_n))$$

in the affine space of dimension $n+1$. Then V_ρ is biregularly equivalent to Ω_ρ.

COROLLARY 3. *Let V be a variety, defined over a field k. The set of points of V where V is normal* (resp. *relatively normal with respect to k*) *is a k-open subset of V.*

Let V^* be the variety derived from V by normalization with reference to the smallest perfect field $k' = k^{p^{-\infty}}$ containing k (resp. with reference to k); let x be a generic point of V over k; let x^* be the corresponding point of V^*, which is generic over k' (resp. over k) on V^*. We may then write $x^* = \phi(x)$, where ϕ is a mapping of V into V^*, defined over k' (resp. over k). Then the points where V is normal (resp. relatively normal) are those where ϕ is defined. As any k'-open set is also k-open, this proves the corollary.

PROPOSITION 9. *Let V be a variety, defined over a field k; let F be a closed subset of V. For F to be k-closed, it is necessary that it should contain all the specializations over k of all its points; it is sufficient that it should contain all the generic specializations over k of all its points, or also that it should be invariant under all isomorphisms over k of a common field of definition $K \supset k$ for its components.*

The necessity of the first condition follows from F-IV$_2$, Th. 4; we first prove that this condition is sufficient. In fact, it implies that, if z is a generic point over K of a component Z of F, the locus Z' of z over $\bar{k}$ is contained in F; as Z is the locus of z over $\bar{K}$, Z' contains Z; as z cannot be in any other component of F than Z, we get $Z' = Z$; thus all components of F are algebraic over k, and then F-IV$_2$, Th. 4, shows that all the conjugates of Z over k must be contained in F. Now we show that the second condition implies the first one. Let x be any point of F and let x' be a specialization of x over k. Then if V is the locus of x over $\bar{k}$, F-IV$_2$, Th. 4, shows that x' must be on a conjugate V' of V over k. Let x'' be a generic point of V' over $\bar{K}$; then x'' is a generic specialization of x over k by F-IV$_2$, Th. 4, and is therefore in F by hypothesis, and x' is a specialization of x'' over $\bar{K}$ and a fortiori over K and so is in F since F is K-closed. Finally the last condition implies the second one; for let x' be a generic specialization over k of a point x in a component Z of F; then the isomorphism of $k(x)$ onto $k(x')$ over k which maps x onto x' can be extended to an isomorphism σ of $K(x)$

onto a field $K^\sigma(x')$, and then x' is on Z^σ by F-IV$_2$, Th. 3, Coroll. 2, and is therefore in F if F is invariant under σ.

PROPOSITION 10. *Let W be a subvariety of a product $U \times V$, with the "projection" U on U; let k be a field of definition for U, V, W. Then the set-theoretic projection of W on U contains an open subset of U; and the union of all such sets is k-open.*

The assumption means that, if (u, v) is a generic point of W over k, u is generic over k on U. Let V_1 be a representative of V on which v has a representative v_1; F_1 being the corresponding frontier, put $V_1' = V_1 - F_1$, so that v_1 is in V_1'; let W_1 be the locus of (u, v_1) over k on $U \times V_1'$. Let V_0 be the projective variety whose part "at finite distance" is V_1; put $F_0 = V_0 - V_1'$; this is a k-closed set on V_0. The set $W_1 \cap (u \times V_1')$ can be written as $u \times X$, where X is either V_1' (in the trivial case $W = U \times V$) or else a $k(u)$-closed subset of V_1'; as v_1 is in X, X is not empty, so that we can choose in it a point w which is algebraic over $k(u)$. Let W' be the locus of (u, w) over $\bar{k}$ on $U \times V_0$, which has the same dimension as U; call n that dimension. Then the set $C = W' \cap (U \times F_0)$ is a $\bar{k}$-closed subset of W', so that all its components are of dimension $\leqq n-1$. As V_0 is complete, the set-theoretic projection C' of C on U is then a $\bar{k}$-closed subset of U. Let a be any point in $U - C'$; as V_0 is complete, there is a point (a, b) on W' with the projection a on U; as a is not in C', b cannot be in F_0 and is therefore in V_1', so that (a, b) is in W_1. Therefore the $\bar{k}$-open set $U - C'$ on U is contained in the set-theoretic projection of W_1 and a fortiori in that of W. The last assertion in our proposition is then an immediate consequence of the sufficiency of the last condition in Prop. 9.

PROPOSITION 11. *Let U, V, W be three varieties and f a mapping of $U \times V$ into W, all defined over a field k. Assume that, for every $a \in U$, f is defined at (a, x) for x generic on V over $k(a)$. Let Ω be the set of those $a \in U$ such that, for x generic over $k(a)$ on V, $f(a, x)$ is generic over $k(a)$ on W. Then Ω is either empty or k-open on U.*

Let r be the dimension of W; for z generic over k on W, let $z_1, \cdots, z_r$ be r algebraically independent elements of $k(z)$ over k; put $z_i = \phi_i(z)$, where ϕ_i is a function on W, defined over k. It is clear that a point z' of W is generic over an overfield K of k if and only if the ϕ_i are all defined at z' and their values $\phi_i(z')$ are independent over K. Let u, x be independent generic points of U, V over k; we may assume that $f(u, x)$ is generic over k on W, since otherwise Ω is empty. Put $f_i = \phi_i \circ f$; Ω is then the set of

those points a on U such that, for x generic over $k(a)$ on V, the $f_i(a,x)$ are all defined and are algebraically independent over $k(a)$.

Take u, x as above; assume that u is not in Ω; we prove that Ω must then be empty. In fact, the assumption on u means that there is a polynomial P with coefficients in $k(u)$ such that

$$P(f_1(u,x),\cdots,f_r(u,x))=0.$$

Write $P=\sum_\nu t_\nu M_\nu(Z)$, where the $M_\nu(Z)$ are monomials (with coefficient 1) in the indeterminates $Z_1,\cdots,Z_r$, and the t_ν are in $k(u)$ and not all 0. Let a be any point of U, and take x' generic over $K=k(a)$ on V. Take a variable quantity λ over $k(u,x)$; extend the specialization $u\to a$ over k to a $\bar{K}$-valued place π of the field $k(u,\lambda)$ such that the elements λt_ν of $k(u,\lambda)$ are all finite and not all 0 at π; call t_ν' the value of λt_ν at π. As $k(u,\lambda)$ and $k(x)$ are independent regular extensions of k, the place π of $k(u,\lambda)$ and the isomorphism of $k(x)$ onto $k(x')$ over k which maps x onto x' make up a specialization of the set of quantities $k(u,\lambda)\cup k(x)$, which can be extended to a place π' of $k(u,\lambda,x)$ at which u, x and the λt_ν have respectively the values a, x' and t_ν'. If the $f_i(a,x')$ are not all defined, a is not in Ω; if they are all defined, they are the values at π' of the elements $f_i(u,x)$ of $k(u,\lambda,x)$. In the latter case, the relation

$$\lambda P(f_1(u,x),\cdots,f_r(u,x))=0,$$

taken at π', gives an algebraic relation between the $f_i(a,x')$ whose coefficients t_ν' are in $\bar{K}$ and are not all 0; this implies that the $f_i(a,x')$ are not independent over $K=k(a)$, so that a is again not in Ω. This shows that, for $u\notin\Omega$, Ω must be empty. From now on, therefore, we may assume that u is in Ω.

We prove now that Ω must contain a k-open set. Since the assumptions and the conclusion of our proposition are not affected if V is replaced by any birationally equivalent variety to V over k (the mapping f being transferred to the latter in an obvious manner), we may take for V an affine variety; put $x=(x_1,\cdots,x_m)$. Then we can write the f_i as

$$f_i(u,x)=P_i(x)/P_0(x),$$

where $P_0,P_1,\cdots,P_r$ are polynomials in the indeterminates $X_1,\cdots,X_m$ with coefficients in $k(u)$, and $P_i(x)\neq 0$ for $0\leqq i\leqq r$. Call $M_\nu(X)$, with $0\leqq\nu\leqq N$, all the monomials in $X_1,\cdots,X_r$ which either are of degree 0 or 1 (i.e. equal to one of the monomials 1, $X_1,\cdots,X_r$) or occur in one at least of the P_i; call $\bar{x}$ the point in the projective space P^N with the homo-

geneous coordinates $(M_\nu(x))$, and call $\bar{V}$ the locus of $\bar{x}$ over k. We may replace V by the birationally equivalent $\bar{V}$; then, writing V, x instead of $\bar{V}$, $\bar{x}$, and calling $(x_0, \cdots, x_N)$ the homogeneous coordinates for x, we see that the $f_i(u,x)$ are expressed as z_i/z_0, with

$$z_i = \sum_{\nu=0}^{N} t_{i\nu} x_\nu \qquad (0 \leqq i \leqq r),$$

where the $t_{i\nu}$ are elements of $k(u)$. If V is contained in any linear subvariety of P^N, then the smallest linear subvariety of P^N which contains V is defined over k; if this is of dimension N', we can express $N - N'$ of the coordinates x_ν linearly in terms of the others, with coefficients in k; thus we may assume that V is not contained in any linear subvariety of P^N.

We may write $t_{i\nu} = \phi_{i\nu}(u)$, where the $\phi_{i\nu}$ are functions on U, defined over k; as z_0 is not 0, we may assume that $t_{00} = 1$. By Prop. 8, the subset U' of U where all the $\phi_{i\nu}$ are defined and finite is k-open. Call n the dimension of V; as n is then the dimension of $k(u,x)$ over $k(u)$, and the $f_i(u,x)$ are independent over $k(u)$, we have $r \leqq n$. Put $z_j = \sum_\nu w_{j\nu} x_\nu$ for $r+1 \leqq j \leqq n$, where the $w_{j\nu}$, for $r+1 \leqq j \leqq n$, $0 \leqq \nu \leqq N$, are $(n-r)(N+1)$ independent variables over $k(u,x)$; call S the affine space of dimension $(n-r)(N+1)$. By F-II$_5$, Prop. 24, the $n-r$ quantities $z_{r+1}/z_0, \cdots, z_n/z_0$ are algebraically independent over the field

$$K = k(u, w, z_1/z_0, \cdots, z_r/z_0).$$

Now take any $a \in U'$; take $\bar{x}$, $\bar{w}$ generic and independent over $k(a)$ on V, S; put $\bar{t}_{i\nu} = \phi_{i\nu}(a)$, $\bar{z}_i = \sum_\nu \bar{t}_{i\nu} \bar{x}_\nu$ for $0 \leqq i \leqq r$, and $\bar{z}_j = \sum_\nu \bar{w}_{j\nu} \bar{x}_\nu$ for $r+1 \leqq j \leqq n$. As $\bar{t}_{00} = 1$, and V is not contained in any linear variety, $\bar{z}_0$ is not 0; therefore, if we put $f_j = z_j/z_0$ for $r+1 \leqq j \leqq n$, the functions $f_1, \cdots, f_n$ on $U' \times S$ are defined at $(a, \bar{w})$ and have the values $\bar{z}_1/\bar{z}_0, \cdots, \bar{z}_n/\bar{z}_0$ respectively. If one assumes that $\bar{z}_1/\bar{z}_0, \cdots, \bar{z}_n/\bar{z}_0$ are algebraically independent over $k(a, \bar{w})$ this implies a fortiori that $\bar{z}_1/\bar{z}_0, \cdots, \bar{z}_r/\bar{z}_0$ are so over $k(a)$, i.e. that $a \in \Omega$. Therefore, if we prove that there is a k-closed subset C of $U' \times S$ such that, with the notations just introduced, the quantities $\bar{z}_1/\bar{z}_0, \cdots, \bar{z}_n/\bar{z}_0$ are algebraically independent over $k(a, \bar{w})$ whenever $(a, \bar{w})$ is not in C, it will follow that Ω contains the set of those points a on U' such that $a \times S$ is not contained in C; and this set will be k-open by Prop. 7. In other words, as long as we merely wish to prove that Ω contains a k-open set, it is enough to prove it for $U' \times S$ and the functions $f_i = z_i/z_0$ for $1 \leqq i \leqq n$ instead of for U and for $f_1, \cdots, f_r$. This means that, writing U instead of $U' \times S$,

it is enough to prove our assertion under the additional assumption $r = n$, the $\phi_{i\nu}$ being now everywhere defined on U, with $\phi_{00} = 1$.

This being now assumed, put $z_{n+1} = \sum_\nu w_\nu x_\nu$, where the w_ν are $N+1$ independent variables over $k(u,x)$. As $k(u,w,x)$ is of dimension n over $k(u,w)$, there is a homogeneous polynomial P, with coefficients in $k(u,w)$ and not all 0, such that $P(z_0, \cdots, z_n, z_{n+1}) = 0$, and P is uniquely determined up to a factor in $k(u,w)$. As $z_1/z_0, \cdots, z_n/z_0$ are algebraically independent, there is at least one term in P where z_{n+1} occurs with a non-zero exponent; after multiplying P with a suitable element of $k(u,w)$, we may assume that the coefficient of this term is 1. Write all the other coefficients in P as $\psi_\rho(u,w)$, where the ψ_ρ are functions on $U \times S^{n+1}$, defined over k. We now prove our assertion about Ω by showing that Ω contains the set of all points a on U such that all the ψ_ρ are defined at $(a, \bar{w})$ for $\bar{w}$ generic on S^{n+1} over $k(a)$; this is a k-open subset of U by Prop. 8 and 7. In fact, let a be a point with that property; take $\bar{x}$ generic over $k(a,\bar{w})$ on V. Put $\bar{t}_{i\nu} = \phi_{i\nu}(a)$, these being all defined, according to our present assumptions; put $\bar{z}_i = \sum_\nu \bar{t}_{i\nu}\bar{x}_\nu$ for $0 \leqq i \leqq n$, and $\bar{z}_{n+1} = \sum_\nu \bar{w}_\nu \bar{x}_\nu$. If we specialize the relation

$$P(z_0, \cdots, z_{n+1}) = 0$$

over the specialization $(\bar{a}, \bar{w}, \bar{x})$ of (u,w,x) with respect to k, we get, since the ψ_ρ are all defined at $(a,\bar{w})$, a homogeneous relation between $\bar{z}_0, \cdots, \bar{z}_{n+1}$ with coefficients in $k(a,\bar{w})$, containing $\bar{z}_{n+1}$ with a non-zero exponent in a term of coefficient 1. This shows that $\bar{z}_{n+1}/\bar{z}_0$ is then algebraic over the field $L(\bar{w})$, where we have put

$$L = k(a, \bar{z}_1/\bar{z}_0, \cdots, \bar{z}_n/\bar{z}_0).$$

Now take $n(N+1)$ independent variables $w_{i\nu}$ over $k(a)$, for $1 \leqq i \leqq n$, $0 \leqq \nu \leqq N$; put $y_i = \sum_\nu w_{i\nu}\bar{x}_\nu$ for $1 \leqq i \leqq n$; what we have proved above shows that, for each i, $y_i/\bar{z}_0$ is algebraic over $L(w_{i0}, \cdots, w_{iN})$, and therefore a fortiori over the field

$$L' = L(w_{10}, \cdots, w_{nN}) = k(a, w_{10}, \cdots, w_{nN}, \bar{z}_1/\bar{z}_0, \cdots, \bar{z}_n/\bar{z}_0).$$

On the other hand, one sees just as before, using F-II$_5$, Prop. 24, that the $y_i/\bar{z}_0$, for $1 \leqq i \leqq n$, are algebraically independent over the field $k(a, w_{10}, \cdots, w_{nN})$; as they are algebraic over L', this implies that L' has at least the dimension n over the latter field, so that the $\bar{z}_i/\bar{z}_0$, for $1 \leqq i \leqq n$, must be algebraically independent over it. But then they must a fortiori be so over $k(a)$, which means that a is in Ω.

This completes the proof of the following statement: the assumptions being again those of Prop. 11, Ω must either be empty or contain a k-open subset of U. Now we prove Prop. 11 by induction on the dimension of U, the conclusion being trivially true if that dimension is 0. Assume that Ω is not empty; put $X = U - \Omega$; we have proved that X is contained in a k-closed subset C of U. Call U_i the components of C; they are algebraic over k, and of dimension $< \dim(U)$. By the induction assumption, $\Omega \cap U_i$ is either empty or a $\bar{k}$-open subset of U_i; in both cases its complement C_i on U_i is a $\bar{k}$-closed subset of U. As X is the union of the C_i, this shows that X is $\bar{k}$-closed. As it is obviously invariant by all automorphisms of $\bar{k}$ over k, it must then be k-closed.

PROPOSITION 12. *Let U be a variety defined over a field k; let F be a closed subset of U. Then, among all the k-closed subsets of U contained in F, there is one maximal set F_0.*

Let K be the smallest common field of definition containing k for all the components of F; let σ run through all the isomorphisms of K over k into the universal domain. As such an isomorphism σ leaves all k-closed sets invariant, every k-closed subset of U which is contained in F is contained in all the sets F^σ and therefore in their intersection F_0; F_0 is closed, since it is the intersection of closed sets; and it is k-closed, by Prop. 9. This proves the proposition.

PROPOSITION 13. *Let U be a variety defined over an infinite field k; let F be a closed subset of $U \times U$. Then there is a point a on U, separably algebraic over k and such that no pair (a', a'') of distinct conjugates of a over k is in F.*

Applying Prop. 12 to $U \times U$, F and the algebraic closure $\bar{k}$ of k, we see that there is a $\bar{k}$-closed subset F_0 of $U \times U$ such that a subvariety of $U \times U$ which is algebraic over k is contained in F if and only if it is contained in F_0; this applies in particular to algebraic points over k on $U \times U$. By replacing F by the union of all conjugates over k of all the components of F_0, we see that it is enough to prove our result in the case in which F is k-closed. We may assume that no component of F is contained in the diagonal of $U \times U$, since the omission of such components does not affect the content of our proposition. Furthermore, we may, in order to prove our proposition, replace U by any k-open subset of U; in view of this, we first replace U by the set of its simple points, and then use Corollary 2 of Prop. 8 to replace U by an affine variety. Thus we may assume that U is a non-singular affine

variety, defined over k, and that F is a k-closed subset of $U \times U$, no component of which is contained in the diagonal of $U \times U$.

Let n and N be the dimensions of U and of the ambient affine space, respectively. The case $n = N$ is trivial, since in that case any rational point of U over k, e.g. 0, would solve our problem; therefore we assume $n < N$. Consider all sets of n linear equations:

$$\sum_{\nu=1}^{N} t_{i\nu} X_\nu = t_{i0} \qquad (1 \leqq i \leqq n), \tag{1}$$

and identify the set (1) with the point $t = (t_{i0}, t_{i\nu})$ in the affine space T of dimension $n(N+1)$. In the space T, we consider the following sets:

(a) Call A the set of those points t for which the left-hand sides of (1) are not linearly independent; as A can be described as the set of zeros of certain determinants, it is k_0-closed, k_0 being the prime field (one could easily see that A is in fact a variety, defined over k_0). Put $T' = T - A$; for $t \in T'$, (1) defines a linear variety $L(t)$ of dimension $N - n$.

(b) Take t generic over k on T; by F-V_1, Th. 1, $U \cap L(t)$ is not empty, and, if u is a point in it, u is algebraic over $k(t)$ and is generic on U over the field $K = k(t_{11}, \cdots, t_{nN})$. As the t_{i0} are then in $K(u)$, we have $k(u,t) = K(u)$, so that $k(u,t)$ is a regular extension of k. Let W be the locus of (u,t) over k on $U \times T$; by F-V_1, Prop. 4, if $t' \in T'$, a point u' is in $U \cap L(t')$ if and only if (u', t') is in W. By Prop. 10, there is a k-closed subset B of T such that $T - B$ is contained in the set-theoretic projection of W on T; then, if $t' \in T - (A \cup B)$, $U \cap L(t')$ is not empty.

(c) Let $P_\rho(X) = 0$, for $1 \leqq \rho \leqq r$, be a set of equations for U with coefficients in k; put $P_{\rho\nu} = \partial P_\rho / \partial X_\nu$. Let D be the subset of $U \times T$ consisting of the points where the matrix

$$\left\| \begin{matrix} t_{i\nu} \\ P_{\rho\nu}(u) \end{matrix} \right\| \qquad (1 \leqq i \leqq n, 1 \leqq \rho \leqq r; 1 \leqq \nu \leqq N)$$

is of rank $< N$; since this can be expressed by the vanishing of determinants, D is a k-closed subset of $U \times T$ (as U is non-singular, it could be shown that D is actually a variety, defined over k). As W is not contained in D, $D \cap W$ is a k-closed subset of W (also, in fact, a variety), so that its components have a dimension $< n(N+1)$. Let D' be the "projection" of $D \cap W$ on T (i.e. the closure of the set-theoretic projection); this is a k-closed subset of T. Let u' be a point in $U \cap L(t')$, for $t' \in T'$; then, if $L(t')$ is not transversal to U at u', (u', t') must be in D and therefore in

$D \cap W$, and t' must be in D'. Therefore, if $t' \in T - (A \cup D')$, $L(t')$ is transversal to U at every point of $U \cap L(t')$.

(d) Let X be any component of F; let (u, v) be a generic point of X over $\bar{k}$. As X is not in the diagonal of $U \times U$, we have $u \neq v$ and may assume for instance that $u_1 \neq v_1$. Take the $t_{i\nu}$ independent over $k(u, v)$ for $1 \leqq i \leqq n$, $2 \leqq \nu \leqq N$; as $n < N$, t will then be in T' for all choices of the t_{i1}, t_{i0}. Determine the t_{i1}, t_{i0} by the condition that $L(t)$ should contain both u and v; this determines them uniquely. As X is at most of dimension $2n - 1$, (u, v, t) is then of dimension $< n(N+1)$ over k; therefore the locus Y of t over $\bar{k}$ is not T. For any $t' \in T'$, assume that $U \cap L(t')$ contains two distinct points u', v' such that (u', v') is in X; then there is ν such that $u_\nu' \neq v_\nu'$, which implies that $u_\nu \neq v_\nu$. It is easily seen that the $t_{i\mu}$, for $1 \leqq i \leqq n$ and all $\mu \neq \nu$ and $\neq 0$, must then be independent over $k(u, v)$, and furthermore that (u', v', t') must be a specialization of (u, v, t) over $\bar{k}$, so that t' is in Y. Therefore, if t' is in T' and is not in the union C of all the varieties Y corresponding in this manner to the components X of F, there cannot be a pair of distinct points (u', v') in $U \cap L(t')$ such that (u', v') is in F. To conjugate components X, X' of F over k, there correspond conjugate varieties Y, Y' over k in T; therefore C is a k-closed subset of T.

Now let $P(t)$ be any polynomial other than 0 in the coordinates of t, with coefficients in k, which is 0 on the union of the k-closed subsets A, B, D' and C of T. As k is infinite, there is on T a rational point t over k such that $P(t) \neq 0$. As t is not in A, it determines a linear variety $L(t)$; as t is not in B, $U \cap L(t)$ is not empty. Take for a any point in $U \cap L(t)$; as t is not in D', $L(t)$ is transversal to U at a, so that a is separably algebraic over k. As all the conjugates of a over k are in $U \cap L(t)$, and as t is not in C, no pair of distinct conjugates a', a'' of a over k can be such that (a', a'') is in F. This completes the proof.

If k is a finite field, the conclusion of Prop. 13 need not be true. In fact, take for U a variety without rational points over k (e.g. the plane non-singular curve $x^4 + y^4 + z^4 = 0$ over the field with 5 elements); q being the number of elements of k, and $(x_1, \cdots, x_n)$ being a representative of a generic point of U over k, call x' the point whose corresponding representative is $(x_1^q, \cdots, x_n^q)$. Then the conclusion of Prop. 13 is false if we take for F the locus of (x, x') over k on $U \times U$.

PROPOSITION 14. *Let V be an affine variety, defined over a field k; let x be a generic point of V over k; assume that the ring $k[x]$ is integrally closed in $k(x)$. Then, if k' is any separably algebraic extension of k, $k'[x]$ is integrally closed in $k'(x)$.*

Put $n = [k' : k]$; as k' is separably algebraic over k, there are n distinct isomorphisms σ of k' into the algebraic closure of k. Each σ can then be extended uniquely to an isomorphism, which we also denote by σ, of $k'(x)$ onto $k'^{\sigma}(x)$ over $k(x)$. Let z be an element of $k'(x)$, integral over $k'[x]$ and therefore also over $k[x]$; then all the z^{σ} are also integral over $k[x]$. If $\xi_1, \cdots, \xi_n$ are n linearly independent elements of k' over k, it is well-known that $\det(\xi_i^{\sigma})$ is not 0; therefore all the z^{σ}, and z among them, can be expressed as linear combinations of the n elements $w_i = \sum_{\sigma} \xi_i^{\sigma} z^{\sigma}$; but these are integral over $k[x]$ and are traces over $k(x)$ of elements of $k'(x)$, so that they are in $k(x)$; as $k[x]$ is integrally closed, the w_i are therefore in $k[x]$, so that z is in $k'[x]$.

THE UNIVERSITY OF CHICAGO.

CORRECTIONS TO THE PAPER "LINEAR GRAPHS OF DEGREE $\leqq 6$ AND THEIR GROUPS."*

By I. N. KAGNO.

D. W. Crowe and Frank Harary in a paper "Linear graphs through seven points . . ." which they are preparing for publication, call attention to a graph which was omitted by the author in his paper mentioned in the above title (this JOURNAL, vol. 68, 1946, pp. 505-520, and vol. 69, 1947, p. 872). The author finds that this was inadvertantly omitted in preparing his paper for publication, and now wishes to call attention to the following corrections to cover this omission.

On page 514, after line 16 add:

$$H'_7 \equiv [ab, ac, ad, ae, af, bc, bd, be, bf, ce, cf].$$

On page 515, after Theorem 3.6 add:

THEOREM 3.6*. *H'_7 has the group* $(abc)\text{all}(def)\text{all}$.

On page 520, Theorem D.11 should read:

$\mathfrak{H}_{28}$ *has the graphs* $P \equiv [\cdot\ \cdot\ \cdot]$ *and* H'_7.

NEW YORK CITY.

* Received February 21, 1955.

ON STRONG SUMMABILITY OF FOURIER SERIES.*

By R. SALEM.

Introduction. Let $f(x) \varepsilon L$ have period 2π and denote by $s_n(x)$ the partial sum of order n of the Fourier series of $f(x)$. Write

$$\phi_x(t) = f(x+t) + f(x-t) - 2f(x).$$

It is now a classical result that, if $f \varepsilon L^r$ $(r > 1)$, then at every point x where

$$\int_0^h |\phi_x(t)|^r \, dt = o(h), \tag{1}$$

(relation which is true for almost all x), one has

$$\sum_{\nu=0}^{n} |s_\nu(x) - f(x)|^q/(n+1) \to 0 \tag{2}$$

for all positive exponents q. See Zygmund [3] and the references quoted there. This theorem has been generalized by Marcinkiewicz [1] and by Zygmund [4] to the case in which one supposes only that $f \varepsilon L$.

In the case $q = 1$, the result can be considered as an extension of the classical Fejér summability theorem, to which it reduces if instead of the average of the absolute values $\sum_0^n |s_\nu - f|/(n+1)$, we consider the average without absolute values $\sum_0^n (s_n - f)/(n+1) = \sigma_n - f$ where σ_n denotes the Fejér sum of order n. Hence the name of "strong summability."

It is natural to ask the question whether the average (2) tends to zero, if instead of considering *all* sums $s_\nu(x)$ $(\nu = 0, 1, 2, \cdots)$, we consider only indices forming a subsequence of the sequence of natural numbers.

The first result in this direction is due to Zalcwasser [2] who proved that, if $f \varepsilon L$,

$$\sum_{k=0}^{n} (s_{k^2} - f)/(n+1) \to 0$$

---

* Received December 27, 1954.

at every Lebesgue point, and in particular at every point of continuity. This result was later extended to indices k^3 or k^4. All proofs are based on number theory methods using the arithmetical properties of the particular kind of sequence involved. Besides, the averages are not taken in absolute value.

In a different direction, some results where the averages are taken with absolute values have been obtained for more general sequences of indices by Zalcwasser and Zygmund but they are only known to hold almost everywhere (even for continuous f), the exceptional set of measure zero depending on the particular sequence $\{n_k\}$ of indices considered.

The main purpose of this paper is to show (in Theorem I) that if $f \varepsilon L^r$ $(r>1)$ and if the condition (1) is satisfied at a point x, then at this point $\sum_{j=1}^{k} |s_{n_j}(x) - f(x)|^q/k \to 0$ for an arbitrarily large exponent q, and for a rather general kind of sequence $\{n_k\}$ which does not increase too rapidly and possesses some weak kind of regularity. Arithmetical properties of the sequence do not enter in the argument.

In the remarks following the proof of Theorem I we show that if $\{n_k\}$ increases rapidly enough, the theorem becomes false. We also show that some hypothesis about the regularity of the sequence can not be avoided.

Theorem II, although not directly connceted with the previous results, is somewhat related to them; its object is to show that, denoting by M_n the maximum of $|s_n(x)|$ with respect to x, there exist continuous functions for which $(M_1 + \cdots M_n)/n$ is unbounded.

THEOREM I. *Let $\{n_k\}$ be an increasing sequence of positive integers satisfying the following conditions:*

1) *There exists a constant A such that $n_k = O(k^A)$*

2) *There exists a constant $\epsilon > 0$ such that $(n_{k+1} - n_k)/n_k > \epsilon/k$*

3) *There exists a lacunary sequence k_ν $(k_{\nu+1}/k_\nu \geqq R > 1)$ such that $n_{k_{\nu+1}}/n_{k_\nu} < B$, B being a constant.*[1]

Let $f(x)$ with period 2π belong to L^s $(s>1)$, and denote by $s_m(x)$ the partial sum of order m of its Fourier Series. Write

$$\phi_x(t) = f(x+t) + f(x-t) - 2f(x).$$

[1] Condition 2) is certainly verified if $\{n_k\}$ is convex, and condition 3), if for a positive c, n_k/k^c decreases.

Then at every point x where $\int_0^\eta |\phi_x(t)|^s\,dt = o(\eta)$ *one has, as* $k\to\infty$,

$$\{|s_{n_1}(x)-f(x)|^r+\cdots+|s_{n_k}(x)-f(x)|^r\}/k\to 0$$

the exponent r being fixed, but arbitrarily large.

Preliminary remarks. a) It is well known that if the theorem is true for the exponent r, it is also true for any smaller exponent. Let q be the exponent complementary to r $(1/q+1/r=1)$. Taking r large enough we have $q<s$, so that we can assume $r\geqq 2$, $1<q\leqq 2$, $f\,\varepsilon\, L^q$ and

$$\int_0^\eta |\phi_x(t)|^q\,dt = o(\eta).$$

b) In the hypothesis 3) about the sequence $\{n_k\}$ we shall assume that $k_\nu = 2^\nu$; the changes in the proof for the general case are trivial.

c) We remark that

$$\int_0^\eta |\phi_x(t)|^s\,dt = o(\eta) \text{ implies } \int_0^\eta |\phi_x(t)|\,dt = o(\eta),$$

hence by a classical result

$$s_n - f = \tfrac{1}{\pi}\int_\delta^\pi \phi_x(t)\sin nt\,dt/t + o(1)$$

as $n\to\infty$, provided that $\delta = O(1/n)$.

Proof of the theorem. We shall assume temporarily that in the hypothesis 2), $\epsilon > 2$, and we shall lift this restriction at the end of the proof.

Consider now an $h=2^\nu$. We shall prove first that $\sum_{j=h}^{j=2h-1} |s_{n_j}-f|^r = o(h)$ as $h\to\infty$. From this the theorem will follow easily.

By remark (c), and since $n_{2h}/n_h < B$ it will be enough to prove that $T=\sum_{j=h}^{2h-1}\left|\int_{\pi/n_h}^\pi \phi_x(t)\sin n_j t\,dt/t\right|^r = o(h)$. For this purpose we shall consider the sum

$$S=\sum_{j=h}^{2h-1}\alpha_j\int_{\pi/n_h}^\pi \phi_x(t)\sin n_j t\,dt/t = \int_{\pi/n_h}^\pi \phi(t)\left(\sum_h^{2h-1}\alpha_j\sin n_j t\right)dt/t,$$

where the coefficients α_j are arbitrary, and where we write $\phi_x(t)=\phi(t)$ since x is fixed and no ambiguity can arise.

We can write $n_h = h^{P+\rho}$ where $P=P(h)$ is an integer and $\rho=\rho(h)$ is such that $0<\rho\leqq 1$. Obviously $P\geqq 0$; also $P\leqq A$. But $P=0$ only if $\rho=1$.

The integrand being the same as in S, we write, if $P>0$,

$$S=\int_{\pi/n_h}^{h\pi/n_h}+\cdots+\int_{\pi h^p/n_h}^{\pi h^p/n_h}+\cdots+\int_{\pi h^{P-1}/n_h}^{\pi h^P/n_h}+\int_{\pi/h^p}^{\pi}$$

$=U_1+\cdots+U_p+\cdots+U_P+V$, say; if $P=0$ we have merely $S=V$, with $\rho=1$.

By a change of variable,

$$U_p=\int_{\pi/h}^{\pi}\phi(h^p\theta/n_h)\,(\sum_{j=h}^{2h-1}\alpha_j\sin(n_jh^p/n_h)\theta)\,d\theta/\theta.$$

We shall find a convenient bound for $|U_p|$. We remark that

$$(n_{j+1}-n_j)h^p/n_h\geqq(n_{j+1}-n_j)h/n_j>(n_{j+1}-n_j)j/2n_j>\epsilon/2>1$$

so that all integers $[n_jh^p/n_h]$ are different (we denote as usual by $[z]$ the integral part of z). To simplify the writing we shall study the integral

$$U=\int_{\pi/h}^{\pi}\phi(\lambda\theta)\,(\sum_{h}^{2h-1}\alpha_j\sin n_j\lambda\theta)\,d\theta/\theta,$$

where $0<\lambda<1$, $(n_{j+1}-n_j)\lambda>1$, and $n_j\lambda\geqq h$. (All three conditions are satisfied by $\lambda=h^p/n_h$.)

We write $\delta_j=(n_j\lambda-[n_j\lambda])/2$, $N_j=(n_j\lambda+[n_j\lambda])/2$, so that $0\leqq\delta_j<\frac{1}{2}$, and $N_j\geqq[h]$. We have $\sin n_j\lambda\theta-\sin[n_j\lambda]\theta=2\sin\delta_j\theta\cos N_j\theta$, and we shall study separately the integral

$$U^*=\int_{\pi/h}^{\pi}\phi(\lambda\theta)\,(\sum_{h}^{2h-1}\alpha_j\sin[n_j\lambda]\theta)\,d\theta/\theta$$

and the difference $U-U^*$.

We have

$$|U^*|\leqq\{\int_{\pi/h}^{\pi}|\phi(\lambda\theta)/\theta|^q\,d\theta\}^{1/q}\{\int^{\pi}|\sum_{h}^{2h-1}\alpha_j\sin[n_j\lambda]\theta|^r\,d\theta\}^{1/r}.$$

Denoting by I, J the two terms of this product, we have

$$I^q=\int_{\pi\lambda/h}^{\pi\lambda}|\phi(t)/t|^q\,dt\cdot\lambda^{q-1}<\lambda^{q-1}\int_{\pi\lambda/h}^{\pi}|\phi(t)/t|^q\,dt.$$

The last integral gives, by a classical process of integration by parts, and owing to $\int_0^{\eta}|\phi(t)|^q\,dt=o(\eta)$, a result which is $o(h/\lambda)^{q-1}$. Hence $I^q=o(h^{q-1})$ and $I=o(h^{1-1/q})$. As for J, since $r\geqq2$ and all $[n_j\lambda]$ are different, it is less, by the theorem of Hausdorff-Young, than the product of $(\sum|\alpha_j|^q)^{1/q}$

by an absolute constant. Hence

$$|U^*| = o(h^{1-1/q})\{\sum_{h}^{2h-1} |\alpha_j|^q\}^{1/q}.$$

Now we consider

$$U - U^* = 2\sum_{j=h}^{2h-1} \alpha_j \int_{\pi/h}^{\pi} \phi(\lambda\theta) \sin \delta_j\theta \cos N_j\theta \, d\theta/\theta$$

and we shall show that $|U - U^*| = \{\sum_{h}^{2h-1} |\alpha_j|\} \cdot o(1)$ as $h \to \infty$.

For this purpose we consider the integral

$$W = \int_a^b \phi(\lambda\theta) \sin \delta\theta \cos m\theta \, d\theta/\theta,$$

where $0 < a < b < 2\pi$, $0 < \lambda < 1$, $0 < \delta < \frac{1}{2}$, $m \geqq [h]$ and we proceed to find an uuper bound for $|W|$.

Write

$$W = \int_{a\lambda}^{b\lambda} \phi(t) \sin (\delta/\lambda)t \cos (m/\lambda)t \, dt/t = \int_{a'}^{b'} \phi(t) \sin (\delta/\lambda)t \cos Mt \, dt/t,$$

where $a\lambda = a'$, $b\lambda = b'$, $0 < a' < b' < 2\pi$, and $M = m/\lambda > m$.

Let $\psi(t) = \phi(t)(\sin \delta/\lambda t)/t = \phi(t)g(t)$. Then $\psi(t) \in L$. As it is well known,

$$\left|\int_{a'}^{b'} \psi(t) \cos Mt \, dt\right| \leqq \tfrac{1}{2}\int_{a'}^{b'} |\psi(t + \pi/M) - \psi(t)| \, dt$$
$$+ \tfrac{1}{2}\int_{a'}^{a'+\pi/M} |\psi| \, dt + \tfrac{1}{2}\int_{b'}^{b'+\pi/M} |\psi| \, dt \leqq \tfrac{1}{2}\int_{a'}^{b'} |\psi(t + \pi/M) - \psi(t)| \, dt$$
$$+ \tfrac{1}{2}(\delta/\lambda)\int_{a'}^{a'+\pi/M} |\phi| \, dt + \tfrac{1}{2}(\delta/\lambda)\int_{b'}^{b'+\pi/M} |\phi| \, dt.$$

We have $\int_E |\phi| dt = \xi(|E|)$ where $\xi \to 0$ with $|E|$, measure of E. Thus

$$\left|\int_{a'}^{b'} \psi(t) \cos Mt \, dt\right| \leqq \tfrac{1}{2}\int_{a'}^{b'} |\psi(t + \pi/M) - \psi(t)| \, dt + (\delta/\lambda)\xi(\pi/M).$$

Now

$$\psi(t + \pi/M) - \psi(t)$$
$$= [\phi(t + \pi/M) - \phi(t)]g(t + \pi/M) + \phi(t)[g(t + \pi/M) - g(t)].$$

Now $|g|$ is bounded by δ/λ, and $|dg/dt|$ by $c(\delta/\lambda)^2$ where

$$c = \max |(d/dt)(\sin t/t)|.$$

Hence

$$\tfrac{1}{2}\int_{a'}^{b'} |\psi(t+\pi/M)-\psi(t)|\,dt$$
$$\leqq (\delta/\lambda)\tfrac{1}{2}\int_{a'}^{b'} |\phi(t+\pi/M)-\phi(t)|\,dt + (\pi/2M)c(\delta/\lambda)^2\int_{a'}^{b'} |\phi|\,dt.$$

Denoting by $\omega(\eta)$ the integral modulus of continuity of the given function f we have, collecting results

$$\left|\int_{a'}^{b'}\psi(t)\cos Mt\,dt\right| \leqq (\delta/\lambda)\xi(\pi/M) + (\delta/\lambda)\omega(\pi/M) + C\delta^2/\lambda^2 M,$$

C being a constant (depending on the value of $f(x)$ only). Since $\delta < \frac{1}{2}$, and $\lambda M = m$, and $M > m \geqq [h]$, we have

$$|W| \leqq C(\xi(\pi/h) + \omega(\pi/h) + 1/h)/\lambda = \mu(h)/\lambda,$$

C being independent of a, b, λ, δ, m; and $\mu(h)$ tending to zero as $h \to \infty$, and depending on h only.

Now, if $\lambda > \mu(h)^{\frac{1}{2}}$ then $|W| \leqq C\mu(h)^{\frac{1}{2}}$. On the other hand, if $\lambda < \mu(h)^{\frac{1}{2}}$

$$|W| < \delta\int_0^{2\pi}|\phi(\lambda\theta)|\,d\theta < (1/2\lambda)\int_0^{2\pi\lambda}|\phi(t)|\,dt = o(1)$$

for $h \to \infty$. Hence $|W| = o(1)$ uniformly as $h \to \infty$ and thus, as stated

$$|U - U^*| = \{\sum_h^{2h-1}|\alpha_j|\}\cdot o(1).$$

Since $\sum|\alpha_j|/h \leqq \{\sum|\alpha_j|^q/h\}^{1/q}$, $|U-U^*| = o(h^{1-1/q})\{\sum|\alpha_j|^q\}^{1/q}$, hence, taking into account the result about U^*,

$$|U| = o(h^{1-1/q})\{\sum_h^{2h-1}|\alpha_j|^q\}^{1/q},$$

and this result is obviously valid also for $|U_1| + \cdots + |U_P|$.

To find a final result for S it remains to appraise V, which is done in a classical way:

$$|V| < \int_{\pi/h}^{\pi}|\phi(t)/t|\cdot\left|\sum_h^{2h-1}\alpha_j\sin n_j t\right|dt$$
$$\leqq \{\int_{\pi/h}^{\pi}|\phi(t)/t|^q\,dt\}^{1/q}\{\int_0^{2\pi}|\sum\alpha_j\sin n_j t|^r\,dt\}^{1/r}$$
$$= o(h^{1-1/q})\{\sum_h^{2h-1}|\alpha_j|^q\}^{1/q},$$ by the Hausdorff-Young theorem.

Collecting results, we have $S = o(h^{1-1/q})\{\sum_h^{2h-1}|\alpha_j|^q\}^{1/q}$. But it is well known that $T^{1/r} = S$ for some α_j satisfying $\{\sum_h^{2h-1}|\alpha_j|^q\}^{1/q} = 1$. Hence

$T^{1/r} = o(h^{1-1/q}) = o(h^{1/r})$, that is to say, $T = o(h)$, as stated. Hence also

$$\sum_{h}^{2h-1} |s_{n_j} - f|^r = o(h).$$

To prove now our theorem it is obvious that it suffices to consider the case $k = 2^{2m} - 1$. Write

$$\sum_{1}^{k} |s_{n_j} - f|^r = \sum_{1}^{2^{m}-1} + \sum_{2^m}^{2^{m+1}-1} + \cdots + \sum_{2^{2m-1}}^{2^{2m}-1}.$$

Consider separately the *first* sum; since $2^m - 1 \sim k^{\frac{1}{2}}$, and since $\int_0^\eta |\phi_x(t)|\,dt = o(\eta)$,

$$\sum_{1}^{k^{\frac{1}{2}}} |s_{n_j} - f|^r = o(k^{\frac{1}{2}} \log^r n_k) = o(k^{\frac{1}{2}} \log^r k) = o(k).$$

Now the sum of the other terms is, by the result just proved,

$$o(2^m) + o(2^{m+1}) + \cdots + o(2^{2m-1}) = o(2^{2m}) = o(k).$$

This completes the proof.

It remains now to get rid of our hyppothesis $\epsilon > 2$. This can be done easily by breaking the sequence $\{n_k\}$ in a finite number of complementary sequences, since there exists an integer C such that $(n_{k+C} - n_k)/n_k > 2/k$.

Remarks on the hypothesis about the sequence $\{n_k\}$. It is certain that if n_k increases *too* rapidly with k, the theorem cannot be true any more. (Consider classical examples of a continuous function whose Fourier Series diverges at a point). But it is not excluded that $n_k = O(k^A)$ can be replaced by a better condition. We wish only to prove here that the theorem is not true for $n_k = O(2^k)$, and not even for $n_k = O(2^{k^\alpha})$ if $\alpha > \frac{1}{2}$. More precisely, the theorem is false if n_k increases sufficiently rapidly to have $\log n_k / k^{\frac{1}{2}} \to \infty$.

The proof is rather simple. Consider a continuous function $f(x)$, with period 2π, and its partial sums s_n at the point $x = 0$. One has

$$s_n = s_n(0) = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t) \sin nt\, dt/t + o(1).$$

Now

$$R_k = (|s_{n_1}| + |s_{n_2}| + \cdots + |s_{n_k}|)/k$$
$$\geqq (\phi_1(u) s_{n_1} + \phi_2(u) s_{n_2} + \cdots + \phi_k(u) s_{n_k})/k,$$

where $\phi_1, \phi_2, \cdots$ are the Rademacher functions. Hence, if we want to prove the unboundedness of R_k it is sufficient to prove the unboundedness—for some $f(t)$—of

$$\int_{-\pi}^{\pi} f(t)\{\phi_1(u)\sin n_1 t + \cdots + \phi_k(u)\sin n_k t\}dt/kt = \int_{-\pi}^{\pi} f(t)H_{k,u}(t)dt.$$

The kernel $H_{k,u}(t)$ depends on two parameters k, u. It will be enough to show that $\int_{-\pi}^{\pi} |H_{k,u}(t)|\,dt$ cannot be bounded independently of k, u. But, if this integral were bounded, we would have

$$\int_0^{\pi} dt \int_0^1 |H_{k,u}(t)|\,du = O(1)$$

independently of k. We know that

$$\int_0^1 |H_{k,u}(t)|\,du > A(1/kt)(\sin^2 n_1 t + \cdots + \sin^2 n_k t)^{\frac{1}{2}}$$
$$> (A/k^{\frac{3}{2}}t)\{|\sin n_1 t| + \cdots + |\sin n_k t|\}.$$

But the integral of this expression with respect to t, in $0, \pi$, is of order $(1/k^{\frac{3}{2}})(\log n_1 + \cdots + \log n_k)$, hence unbounded if $\log n_k/k^{\frac{1}{2}} \to \infty$.

If we come now the condition of regularity (2) of our theorem, we shall show that *some* condition of this kind is necessary to prove the theorem.

We shall base the proof of this remark on the following lemma

LEMMA. *Consider the integral*

$$J_{n,p} = \int_0^{\pi/p} |\sin(n+1)\theta + \cdots + \sin(n+p)\theta|\,d\theta/p\theta$$

(in which we think of n, p, and n/p as being large); this integral is larger than $A\log(n/p)$, A being a positive constant.[2]

Proof. We have

$$J_{n,p} = \int_0^{\pi/p} |\cos(n+p+\tfrac{1}{2})\theta - \cos(n+\tfrac{1}{2})\theta|\,d\theta/\{2p\theta\sin(\theta/2)\}$$
$$> \int_0^{\pi/p} |2\sin p(\theta/2)\sin(n+(p+1)/2)\theta|/p\theta^2$$
$$= \int_0^{\pi} |2\sin(t/2)\sin(n/p+\tfrac{1}{2}+1/2p)t|\,dt/t^2 > A\log(n/p).$$

Take now the sequence n_k in the following way. $n_k = 2^{pv}$ for $k = 2^v$, p being a fixed integer. For $k = 2^v + h$ where $h = 1, 2, \cdots, 2^v - 1$ $n_k = 2^{pv} + h2^{v(p-2)}$.

Obviously $n_k = O(k^p)$.

---

[2] This has certainly been known to many authors.

Let now $f(x)$ be continuous, and s_n be the partial sum of order n for $x=0$.

Let $k=2^\nu$. We have

$$(|s_1|+|s_2+\cdots+|s_{2^{\nu+1}-1}|)/(2^{\nu+1}-1)$$
$$>(|s_{2^\nu}|+\cdots+|s_{2^{\nu+1}-1}|)/(2^{\nu+1}-1).$$

Hence, to prove unboundedness, it is enough to consider the integral

$$\int_{-\pi}^{\pi} f(t)\{\sin k^p t+\sin(k^p+k^{p-2})t+\sin(k^p+2k^{p-2})t$$
$$+\cdots+\sin(k^p+k^{p-1}-k^{p-2})t\}dt/kt,$$

and to prove the unboundedness of

$$\int_0^{\pi}|\sin k^p t+\sin(k^p+k^{p-2})t+\sin(k^p+2k^{p-2})t$$
$$+\cdots+\sin(k^p+k^{p-1}-k^{p-2})t|\,dt/kt,$$

or, setting $k^{p-2}t=\theta$, the unboundedness of

$$\int_0^{k^{p-2}\pi}|\sin k^2\theta+\sin(k^2+1)\theta+\cdots+\sin(k^2+k-1)\theta|\,d\theta/\theta,$$

which is $>A\log k$, by the Lemma.

We could as well have taken for $k=2^\nu+h$ and $h=1,2,\cdots,2^\nu-1$, $n_k=2^{p\nu}+[h2^{\nu(p-1-\epsilon)}]$. In all those examples $(n_{k+1}-n_k)k/n_k$ does not remain above a positive number.

THEOREM II. *Let $f(x)$ be continuous, with period 2π, $s_n(x)$ be the partial sum of order n of its Fourier Series. Let M_n denote the maximum of $|s_n(x)|$ for $0\leqq x\leqq 2\pi$. There exists continuous functions for which $(M_1+M_2+\cdots+M_n)/n$ is unbounded.*

Proof. Write, D_n denoting the Dirichlet kernel,

$$T(m,p,x)=(s_{m+1}(x)+s_{m+2}(x)+\cdots+s_{m+p}(x))/p$$
$$=\tfrac{1}{\pi}\int_0^{2\pi} f(t)\{D_{m+1}(x-t)+\cdots+D_{m+p}(x-t)\}dt/p,$$

and denote by $L(m,p,\theta)$ the kernel $(1/p)[D_{m+1}(\theta)+\cdots+D_{m+p}(\theta)]$.

Let n be given, and k the integer such that $2k^2\leqq n<2(k+1)^2$. One has

$$(M_1+\cdots+M_n)/n$$
$$>(M_1+\cdots+M_{2k^2})/2(k+1)^2>(M_{k^2+1}+\cdots+M_{2k^2})/2(k+1)^2.$$

It will then be sufficient to prove the unboundedness of

$$R_k = (M_{k^2+1} + \cdots + M_{2k^2})/k^2.$$

Let $x_j = j2\pi/k$ $(j = 0, 1, \cdots, k-1)$. Denote by $\phi_0(u), \phi_1(u), \cdots$ the Rademacher functions. Then, obviously, for any value of u,

$$(1/k)(M_{k^2+1} + \cdots + M_{k^2+k}) \geqq \phi_0(u) T(k^2, k, x_0)$$
$$(1/k)(M_{k^2+k+1} + \cdots + M_{k^2+2k}) \geqq \phi_1(u) T(k^2+k, k, x_1)$$
$$(1/k)(M_{k^2+k(k-1)+1} + \cdots + M_{2k^2}) \geqq \phi_{k-1}(u) T(k^2+k(k-1), k, x_{k-1}).$$

Hence

$$\begin{aligned} R_k &\geqq (1/k)\{\phi_0(u) T(k^2, k, x_0) + \phi_1(u) T(k^2+k, k, x_1) \\ &\qquad + \cdots + \phi_{k-1}(u) T(2k^2-k, k, x_{k-1})\} \\ &= (1/\pi k) \int_0^{2\pi} f(t)\{\phi_0(u) L_{k^2,k}(t-x_0) + \phi_1(u) L_{k^2+k,k}(t-x_1) \\ &\qquad + \cdots + \phi_{k-1}(u) L_{2k^2-k,k}(t-x_{k-1})\} \\ &= \tfrac{1}{\pi} \int_0^{2\pi} f(t) H_{k,u}(t)\, dt \text{ say.} \end{aligned}$$

The argument already used above shows that it is sufficient to prove the unboundedness of

$$\int_0^{2\pi} dt \int_0^1 |H_{k,u}(t)|\, du > \int_0^{2\pi} (L^2_{k^2,k}(t-x_0) + \cdots)^{\frac{1}{2}} dt/k.$$

But the last integral is larger than

$$k^{-1} \sum_{j=0}^{k-1} \int_{x_j-\pi/k}^{x_j+\pi/k} |L_{k^2+jk,k}(t-x_j)|\, dt = k^{-1} \sum_{j=0}^{k-1} \int_{-(\pi/k)}^{\pi/k} |L_{k^2+jk,k}(\theta)|\, d\theta,$$

and by the last lemma one has

$$\int_{-(\pi/k)}^{\pi/k} |L_{k^2+jk,k}(\theta)|\, d\theta > C \log(k+j) \geqq C \log k.$$

Hence for suitable choice of the bounded function $f(t)$ (depending on k) $R_k \geqq A \log k$, which, by a classical theorem, proves our result.

More precisely, $\omega(n)$ being any function increasing less rapidly than $\log n$, there is a continuous $f(x)$ such that

$$(1/\omega(n)) \cdot (M_1 + M_2 + \cdots + M_n)/n$$

is unbounded.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY.

BIBLIOGRAPHY.

[1] J. Mazcinkiewicz, "Sur la sommabilité forte des séries de Fourier," *Journal of the London Mathematical Society*, vol. 14 (1939), pp. 162-168.

[2] Z. Zalcwasser, "Sur la sommabilité des séries de Fourier," *Studia Mathematica*, vol. 6 (1936), pp. 82-88.

[3] A. Zygmund, *Trigonometrical Series*, Warszawa-Lwów, 1935, p. 238.

[4] ———, "On the convergence and summability of power series on the circle of convergence (II)," *Proceedings of the London Mathematical Society*, vol. 47 (1942), pp. 326-350.

ERRATA.

P. Hartman and A. Wintner, "Asymptotic integrations of linear differential equations," this JOURNAL, vol. 77, pp. 45-86.

On page 62, formula (67), and on page 72, formula (119), read $\epsilon(a)$ in place of the factor $(\epsilon(j)+\epsilon(a)-1)$ in the exponent of t.

On page 63, formula (70), read $>$ instead of $<$ (twice); in place of the two lines following (70), read "In this case, $y(t)$ is unique."

On page 64, line 11, read [6] in place of [5].

On page 66, formula (80), read $(b(q)-k)$ in place of the factor $(b(q)-h)$.

On page 68, formula (91), read $(\epsilon(a)-\epsilon(j))$ in place of the factor $(\epsilon(a)-1)$ in the exponent of t.